IMPLEMENTACION DE LA RED PRIVADA VIRTUAL (VPN) A LAS SUCURSALES Y USUARIOS EXTERNOS DE LA EMPRESA HARDSOFT S.A

YUDY YOHANNA PRIETO CRISTANCHO

UNIVERSIDAD LIBRE
FACULTAD DE INGENIERIA
DEPARTAMENTO INGENIERIA DE SISTEMAS
CENTRO DE INVESTIGACIONES FACULTAD DE INGENIERIA
BOGOTA D.C.
2011

IMPLEMENTACION DE LA RED PRIVADA VIRTUAL (VPN) A LAS SUCURSALES Y USUARIOS EXTERNOS DE LA EMPRESA HARDSOFT S.A

YUDY YOHANNA PRIETO CRISTANCHO

TRABAJO DE GRADO

Director
Ing. ALVARO ROJAS DAZA

UNIVERSIDAD LIBRE
FACULTAD DE INGENIERIA
DEPARTAMENTO INGENIERIA DE SISTEMAS
CENTRO DE INVESTIGACIONES FACULTAD DE INGENIERIA
BOGOTA D.C.
2011

Nota de aceptación

_____
_____
_____
_____
_____

_____
Firma del presidente de jurado

_____
Firma del jurado

_____
Firma del jurado

AGRADECIMIENTOS

Los autores expresan sus agradecimientos a:

A Dios por brindarnos la salud, inteligencia, fortaleza, perseverancia para seguir adelante sin importar los obstáculos.

A mis padres Edgar Humberto Prieto González y Carmenza Cristancho y mis hermanos por apoyarme incondicionalmente a cumplir mi sueño de ser Ingeniera de Sistemas de la Universidad Libre, por el amor y la paciencia que me tuvieron a pesar de mis altibajos académicos.

DEDICATORIA

Dedicado este proyecto a los Docentes los cuales han entregado sus esfuerzos, conocimientos y buenos deseos para hacer de nosotros unos profesionales preparados y aptos para enfrentar un largo camino profesional.
Dedicado especialmente a nuestras familias y a Dios, las cuales han sido un gran apoyo para luchar y seguir adelante en esta ardua labor de Ingenieros de la Universidad Libre, superando los obstáculos y desavenencias que vivimos a diario durante el proceso académico.

TABLA DE CONTENIDOS

LISTA DE TABLAS

LISTA FIGURAS

GLOSARIO

Ancho de Banda: La cantidad de datos que se pueden transmitir en una cantidad de tiempo determinada. En el caso de la banda ancha digital, en general se expresa en bits por segundo (bps). En el caso de la banda ancha analógica, se expresa en ciclos por segundo, o Hertz (Hz).

Autenticación: Proceso de confirmar la identidad de una entidad de sistema (un usuario, un proceso, etc).

Backbone: Enlace de gran caudal o una serie de nudos de conexión que forman un eje de conexión principal. Es la columna vertebral de una red. Por ejemplo, NSFNET fue el backbone, la columna o el eje principal de Internet durante muchos años.

Cable Directo de Ethernet Cableado UTP en el que el orden de los pines en uno de los extremos sigue el orden de pines 568a y el otro extremos del cable sigue el mismo orden 568a. Se utiliza cuando se conecta una computadora o router a un switch.

Datagramas: son paquetes de información.

Dirección de Broscast: Dirección que pretende representar una transmisión desde un dispositivo a todos los dispositivos en función de la dirección de broadcast especificada.

Dirección de Destino: Dirección a la cual se dirigen los datos.

Dirección de Origen: En comunicaciones y networking, el origen de un canal de comunicaciones.

Dirección de Red: Dirección de capa de red que se refiere a un dispositivo de red lógico, más que físico.

Dirección Física: Dirección de capa data-link, por ejemplo una dirección MAC.

Dirección de Host: Dirección de un host de red. Cuando se habla de direcciones de host, por lo general se habla de la dirección de la capa de red.

Dirección IP: Número exclusivo que utilizan los dispositivos a fin de identificarse y comunicarse entre ellos en una red de computadoras utilizando el estándar de protocolo de Internet (IP).

Dispositivos Intermediarios: Dispositivo que conecta en forma directa con las terminales de usuario final a otras redes. El router es un ejemplo de dispositivo intermediario.

Dominio de Broadcast: Red lógica compuesta por todas las computadoras y dispositivos de red a los que se puede acceder mediante el envío de un frame a la dirección de broadcast de la capa data-link.

Encriptación: Herramienta que permite ocultar el significado de los mensajes a otras partes que no sean el emisor y el receptor de dicha información, utilizando los distintos sistemas de cifrado.

Extranet: Una extranet es una red privada que usa los protocolos de Internet y el sistema público de telecomunicaciones para compartir, de modo seguro, parte de la información de un negocio o las operaciones con proveedores, vendedores, socios, clientes u otro tipo de negocios. Una extranet puede ser considerada como parte de la intranet de una compañía que se amplía a usuarios que están fuera de la empresa.

Gateway por Defecto: Dispositivo de una red que sirve como punto de acceso a otra red. El default Gateway es utilizado por un host cuando la dirección de destino de un paquete IP pertenece a algún lugar fuera de la subred local.

Host: Dispositivo que comunica a través de una red.

I**PV4**: Abreviatura de protocolo de Internet versión 4. Es la versión actual del Protocolo de Internet.

Máscara de Subred: La función de una máscara de subred consiste en identificar la parte de la red, de la subred y del host de una dirección IP. Las máscaras de subred sirven para dividir la red y separar una red grande o sumamente grande en segmentos, o subredes, más pequeños, eficientes y manejables.

Paquete: Estructura de datos con una cabecera que puede estar o no lógicamente completa. Más a menudo, se refiere a un empaquetamiento físico de datos que lógico. Se utiliza para enviar datos a través de una red conmutada de paquetes.

Protocolo de Internet (IP): Protocolo de capa de red en la pila TCP/IP que brinda un servicio de internetworking no orientado a conexión. El IP suministra características de direccionamiento, especificación de tipo de servicio, fragmentación y ensamblaje y seguridad.

Proveedor de Servicios de Internet (ISP): Un ISP es una compañía que brinda acceso a Internet a individuos o empresas.

Puertos: Normalmente los puertos se utilizan para identificar un determinado proceso o servicio en una computadora. Cuando un dispositivo remoto desea acceder a cierto servicio, por ejemplo, dirige esos datos a un puerto determinado que identifica el tipo de servicio que quiere usar el dispositivo

PSI: Proveedores Independientes de Servicio.

Red: Es una colección de estándares, basada en dispositivos que encadenan todo lo referente a la compañía, como computadoras de escritorio, servidores y recursos, sin sacrificar velocidad, costo o maniobrabilidad.

Red de Área Local (LAN): El término de área local (LAN) hace referencia a una red local, o a un grupo de redes locales interconectadas, que están bajo el mismo control administrativo.

Router: Dispositivo de capa de red que usa una o más métricas para determinar la ruta óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes desde una red a otra basándose en la información de la capa de red.

Servidor WEB: Servidor que responde a solicitudes http con datos de respuesta http. El servidor Web también aloja la estructura de directorio de los sitios Web y sus imágenes asociados, y otros archivos de medios.

Tabla de Enrutamiento: Tabla almacenada en la memoria de un router o algún otro dispositivo de networking que guarda un registro de las rutas a destinos particulares de la red. El router utiliza esta lista de redes para determinar donde enviar los datos.

Topología Física: La topología física de una red hace referencia a la configuración de cables, computadoras y otros periféricos.

Topología Lógica: Mapa de los dispositivos de una red y cómo se comunican entre ellos. Muestra el flujo de datos en una red.

Túnel: Técnicas de encapsulado del tráfico**.**

Virus informático: Es un programa creado especialmente para invadir ordenadores y redes y crear el caos. El daño puede ser mínimo, como que aparezca una imagen o un mensaje en la pantalla, o puede hacer mucho daño alterando o incluso destruyendo ficheros.

RESUMEN

Las redes son un factor crítico para las empresas, pues a partir de ellas se puede transmitir información vital de forma segura, envío y recepción de datos en tiempo real, reducción de costos para la empresa y comunicación desde cualquier punto del mundo, superando la barrera de las conexiones locales y permitiendo la conectividad de su personal y oficinas en otros edificios, ciudades e incluso países. En la actualidad gran parte de las entidades y empresas presentan una estructura distribuida, disponiendo de oficinas y sedes en distintos puntos geográficos, permitiendo la comunicación entre ellas ya sea mediante una conexión punto a punto, Frame Relay o RDSI, estas aunque brindan gran seguridad porque la información viaja a través de un canal dedicado, son un poco costosas y exigen inversión tanto de Hardware como de Software, mientras q las VPN son mucho más económicas pues la emisión y recepción de datos se hace mediante la utilización de canales públicos como internet.

Hardsoft es una empresa en desarrollo, por lo tanto quiere una solución segura, eficiente y económica para permitir la comunicación de sus oficinas remotas y usuarios externos con la sede principal, sin invertir tanto en hardware, software y en servicios de telecomunicaciones. Las Redes Privadas Virtuales (VPN) son una solución económica, fiable y segura para la comunicación con usuarios externos a los aplicativos de la sede principal como la intranet, o la utilización de dispositivos periféricos, videoconferencias, manejo y modificación de datos, entre otras funcionalidades que se pueden hacer desde cualquier punto sin necesidad de estar físicamente en la sede principal de Hardsoft S.A.

El diseño de un prototipo de Red Virtual Privada VPN para la empresa HardSorf S.A consiste en utilizar un canal de comunicación público como internet para la comunicación privada con oficinas remotas, usuarios externos como proveedores, clientes y empleados remotos, empleando una técnica de tunneling la cual encapsula un protocolo de red sobre otro creando un túnel dentro de una red de computadores, el establecimiento de este túnel se implementa incluyendo una PDU determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al lado del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada, por tal motivo los datos son encriptados de forma tal que son ilegibles para los extraños.

El principal objetivo de una VPN es conseguir una red a un costo asequible en infraestructura, mantenimiento y seguridad para toda la información transmitida, permitiendo la interconexión entre distintas sedes eliminado la necesidad de utilizar líneas dedicadas entre dos puntos, la cual es una solución muy costosa y dependiente del operador, por otro lado brindar seguridad a través de protocolos de encriptación permitiendo la transmisión de datos con los proveedores, clientes, oficinas remotas de forma segura y acceso rápido a todos los servicios de intranet y otros aplicativos empleados por la empresa para el manejo de datos garantizando la autenticación y autorización a los distintos niveles de acceso que

existan; la integridad de los datos para que no sean alterados y confidencialidad de dichos datos para evitar que sean manipulados o leídos por terceros.
La VPN es capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no están autorizados, además muestra registros estadísticos que muestra quien tuvo acceso a cual información y cuando.
La utilización de una Red Virtual Privada para la empresa Hardsoft S.A además de proteger las comunicaciones de usuarios externos especialmente, permite optimizar los recursos utilizando una única línea para el acceso a internet sin necesidad de emplear las conexiones punto a punto, además garantiza seguridad en todo momento para que los datos sean fiables permitiendo que solamente el emisor y receptor legitimo del mensaje puedan verla en su estado normal.
La adecuación de topologías virtuales VPN permitirán la instalación de nuevas sedes o centros remotos de forma rápida y transparente al usuario sin afectar de alguna forma sus sistemas o redes y sin grandes inversiones que afecten el bolsillo de Hardsoft S.A.

1. INTRODUCCION

La evolución de las redes y del desarrollo tecnológico en las áreas de voz, video y datos, requiere establecer una comunicación eficiente y productiva entre los elementos de la organización a fin de lograr a través de la tecnología, la optimización de la empresa; reduciendo costos, ofreciendo un mejor servicio tanto a los usuarios locales como externos, buscar e implementar nuevas formas de trabajo y tener información más oportuna, rápida y acertada. Esta evolución juegan un rol importante en el uso y aplicaciones de la tecnología, ya que cada vez más las empresas y usuarios, demandan, para las interacciones dentro y fuera de su negocio, aplicaciones Multimedia las cuales requieren de estructuras de Software, Hardware y Ancho de Banda más amplios.
La estructura y topología de estas redes, requieren la demanda de nuevas aplicaciones y conexiones de acceso remoto eficiente, seguro y conveniente para los usuarios externos que permita la transmisión de Vídeo sobre demanda VoD, Telefonía IP V/IP, Videoconferencia, aplicaciones Multimedia, comercio electrónico, acceso a Internet a Altas velocidades ADSL, entre otras, mejorando el tiempo en los procesos, reducción de costos, ofreciendo un mejor servicio y la obtención de información más oportuna y acertada sin importar el lugar y la distancia.

La VPN o Red Virtual Privada es una tecnología que permite la extensión de una red local sobre un canal público “internet”, permitiendo la conexión de usuarios externos desde su casa u otro lugar geográfico a los aplicativos o el mismo servidor de la empresa para verificar o manipular información interna garantizando la autenticación, integración y confidencialidad de toda la información.

La principal motivación del uso y difusión de la VPN Red Virtual Privada en Hardsoft S.A es la reducción de costos directos en implementación de canales privados como en hardware y servicios de telecomunicaciones sin importar la ubicación de sus oficinas. Cada usuario remoto de la red puede comunicarse de manera segura y confiable utilizando internet para conectarse a su red privada local. Las VPNs pueden adaptarse a más usuarios y diferentes lugares gracias a la escalabilidad que tiene sobre las redes dedicadas.
Otras ventajas de esta tecnología para la empresa Hardsoft S.A son la reducción de tiempos y costos de transporte para los usuarios remotos, mejora de la productividad de la empresa, simplificación de la topología empresarial, proveer a los usuarios remotos facilidades de telecomunicaciones, permitir un mejor uso de las redes con un buen ancho de banda y la posibilidad de encontrar oportunidades de negocio a nivel global.

PLANTEAMIENTO DEL PROBLEMA

DESCRIPCION DEL PROBLEMA

Hardsoft es una empresa que vende y compra partes de computadores nuevas o remanofacturadas dependiendo la necesidad y presupuesto del cliente; algunas de las piezas son fabricadas por el personal de la empresa y otras son compradas por proveedores nacionales y extranjeros. Hardsoft S.A cuenta con una única LAN que comunica y comparte la información entre los computadores y comparten dispositivos periféricos. La conexión a internet se realiza a través de un servicio de banda ancha ADSL. La empresa cuenta con servidores de correo electrónico, transferencia de datos, almacenamiento de archivos y acceso a la intranet de la empresa.
Gracias a la creciente demanda de sus servicios, Hardsoft se ha visto en la necesidad de contratar más personal y jerarquizar la empresa en departamentos para darle mayor orden a la asignación de tareas, pese a eso, se deben alquilar mas oficinas para satisfacer sus necesidades crecientes y obtener mayor comodidad y flexibilidad en el lugar de trabajo.
El nuevo desafío de Hardsoft es administrar la entrega de información y servicios a todos los empleados de la empresa y garantizarles que puedan tener acceso a todos los servicios, información y aplicaciones independientemente de cuál sea su ubicación, para ello, es necesario implementar una WAN que permita comunicar entre sí a todas las oficinas o sucursales que se encuentren distantes a la sede central.

La empresa desea proporcionar a los empleados los mejores servicios de red que le permita trabajar con un alto nivel de eficiencia y fomentar el trabajo a distancia con el fin de aumentar la productividad y reducir costos de implementación de redes.
Internet es una opción llamativa de conexión a WAN, ya que es económica pero tiene inconvenientes con la seguridad y privacidad, por lo tanto, se van a combinar con las Redes Privadas Virtuales (VPN), la cual permitirá conectarse con los empleados y las otras oficinas de manera sencilla y segura a través de internet.

Cuando se habla de emplear internet como el medio de transmisión de datos, los empresarios se hacen muchas preguntas referentes a esta forma de transmisión, tales como ¿Sera seguro?, Sera más vulnerable el envío de datos a través de internet, que si viajaran por una red interna o un canal dedicado de la empresa?, se mantendrá la confidencialidad de la información en el momento de salir y llegar a su destino?
Nuestro principal objetivo es satisfacer la necesidad de comunicación de la compañía Hardsoft S.A hacia las otras oficinas o usuarios externos de forma segura y económica, empleando internet como un medio de transmisión con un

protocolo de túnel, el cual encapsula los datos antes de ser enviados de manera cifrada, y garantiza que todos los datos que son transportados por este medio no podrán ser modificados o manipulados.
La VPN o Red Privada Virtual brinda una conexión segura a un bajo costo, ya que la red física es publica y los datos son protegidos mediante un protocolo de túnel, el cual cifra los datos que se transmiten desde un lado de la VPN a otra, impidiendo que la información sea comprensible cualquiera que no se encuentre en los extremos de las VPNs. Este tipo de tecnología no requiere de una línea dedicada, aunque esta brinda mayor seguridad porque está viajando por un canal privado, es muy costosa y no puede conectar dos redes de área local remotas.

SISTEMATIZACION DEL PROBLEMA

- ¿Cuál será el mejor servicio de conectividad que se implementara en la empresa Hardsoft S.A?
- ¿Qué protocolo de seguridad se estudiara para el diseño de la VPN según la facilidad, mantenimiento y tipos de clientes soportados?

FACTIBILIDAD

ECONOMICA

El diseño de una Red Privada Virtual en la empresa Hardsoft S.A es una alternativa económica para el acceso remoto en ambiente corporativo donde empleados, clientes, proveedores pueda intercambiar información de forma segura desde cualquier lugar del mundo a través de internet sin la necesidad de utilizar canales dedicados que son muy costosos.

Las principales razones para adoptar esta solución son fundamentalmente los costes en cuanto a la infraestructura, mantenimiento y seguridad de la información para permitir la comunicación de los usuarios remotos (clientes, proveedores, empleados externos) desde cualquier lugar del mundo.

- Infraestructura: Resulta más económico emplear una infraestructura pública que desplegar una red físicamente privada. Si empleamos una conexión publica estaríamos reduciendo notablemente costos en cuanto facturas a Proveedores de Internet (ISP), cableado, enrutadores.
- Mantenimiento: Para un optimo funcionamiento de las redes se debe efectuar frecuentemente mantenimiento a los elementos que conforman la red, por ejemplo las conexiones locales, WIFI, conexión con el proveedor, hardware y software, en el caso de una red privada los costos serian mayores ya que se debe hacer una revisión

Tabla 1. Presupuesto de Infraestructura Física – Suministros

HARDSOFT S.A

PRESUPUESTO DE INFRAESTRUCTURA FISICA - SUMINISTROS

IMPLEMENTOS	DESCRIPCION	V. UNITARIO	Cantidad	V.TOTAL
HARDWARE				
Definir entorno de la red				
Cable UTP	CAT. 5: Ancho de Banda de 100 Mhz, distancia de hasta 100 Estándares: UL444/UL1581, TIA/EIA 568B.2	246,000 (305 mt)	1000 mt	806.557
Tarjeta Ethernet	Adaptador PCI. Ethernet 10Base-T, Ethernet 100Base-TX. Vel de Transferencia 100 Mbps. Capacidad Duplex, ROM de iniciacion, Negociacion Automatica. Plug and Play. Ranuras compatibles: 1 x PCI. Conector RJ45	50.000	38	1.900.000
Dispositivos de conexión				
Router	Router Modular: Permiten la conexión a redes de cualquier tipo (ADSL2+, VDSL2, Gigabit, E1/T1, Wifi, 3G, etc.), conexión a redes públicas analógicas o digitales (BRI/PRI)). Interfaces Ethernet 10/100/1000. Seguridad (WEP/WPA/WPA2).	4.200.000	3	12.600.000
Switch	Modular. Velocidad de 10/100/1000. 0 puertos 10BASE-T/100BASE-TX/1000BASE-T; puerto de alimentación RPS (-48 VDC); puerto de consola RJ-45; 2 puertos de apilamiento dedicados; 1 ranura para módulo opcional. Seguridad: RADIUS; autenticación PAP/CHAP/EAPoL (EAP sobre LAN)	3.000.000	3	9.000.000
Servidor	Dell: Intel® Xeon® X3440 (8MB Caché, 2.53 GHz, Turbo, HT), Memoria de 16GB (4X4GB), 1333Mhz, Dual RankedUDIMM, RAID 5 - PERC S100 (SATA Software RAID Integrado) soporta 3 a 4 Disco Duros , Disco duro SATA 250GB 7.2K RPM 3Gbps 3.5 pulgadas Cabled, Broadcom® 5709 de puerto doble, Gigabit Ethernet, con TOE/iSCSI, PCIe x4 ,	1.981.897	1	1.981.897
Impresoras	Matriz de Punto Carro Angosto	1.200.000	4	4.800.000
	Laser Color	600.000	5	3.000.000
	TOTAL INFRAESTRUCTURA FISICA			**34.088.454**

Tabla 2. Presupuesto para Diseño e Implementación

HARDSORF S.A
PRESUPUESTO PARA DISEÑO E IMPLEMENTACION

Fase	Descripción	Costo Unitario	Unidades	Total
SOFTWARE				
Sistemas Operativos	Licencia Windows XP	270.000	20	5.400.000
	Licencia Windows Vista	250.000	18	4.500.000
	Licencia Windows Server 2003	420.000	2	840.000
Protocolo de Enrutamiento	Protocolo OSPF	300.000	3	900.000
VPN	Configuración del servidor y clientes VPN	500000	1	500000
	SUBTOTAL SOFTWARE			**1214.000**

Tabla 3. Presupuesto Diseño e Implementación

DISEÑO E IMPLEMENTACION		
FASE DE DISEÑO	Planeamiento de la red. Diseño global y local de la red	525.000
	Estudio de restricciones físicas y requerimientos de los usuarios	700.000
	Definir entorno de hardware y software	2.800.000
FASE DE IMPLEMENTACION	Direccionamiento IP de las Sedes	200.000
	Preparación del local de instalación e instalación de la red. Instalación de la red LAN en cada sede.	500.000
	Configuración de los Dispositivos de conexión (Router, servidor)	250.000
	Configuración de los Equipos de cada sede	50.000
FASE FINAL	Capacitación de los empleados y personal de sistemas	450.000
	Administración de Red (Mantenimiento Continuo - Solución Integrada de Problemas) Semestral	500.000
	SUBTOTAL DISEÑO E IMPLEMENTACION	**5.975.000**
	COSTO TOTAL	**16.715.000**

TECNICA

Mediante la implementación de la Red Privada Virtual brindar los recursos necesarios como conocimientos, habilidades, experiencia, manejo y especificaciones técnicas de esta tecnología a los usuarios, la cual permitirá que la utilización sea fácil y compresible para ellos. Mejora del sistema actual.

OPERATIVA

La adecuación de una Red Privada Virtual en la empresa Hardsoft S.A es un sistema de fácil uso para los usuarios locales y externos, ya que solo requiere de una autenticación y validación de datos para poder ingresar a la información de la empresa, lo cual no generaría un mal uso o fallas en el sistema.

Al momento de implementar esta tecnología debemos establecer si es aceptable por los empleados, que resultados producirá para la empresa y los usuarios externos, la productividad de los empleados mejorara, los clientes se beneficiaran, producirá efectos positivos en algunas o todas las áreas de Hardsoft S.a.

METODOLOGIA

Se realizo una investigación descriptiva y observacional para determinar y validar una estrategia de mejoramiento para la empresa Hardsoft S.A. Para ello se realizaron las siguientes actividades:

- Utilizando la observación y la experimentación, establecer y clasificar los datos con el fin de obtener el propósito del estudio.
- Sistematización de los métodos y de las técnicas necesarias para llevarla a cabo el desarrollo de la red.
- Con base en los datos obtenidos, analizarlos, interpretarlos para alcanzar los objetivos propuestos.

OBJETIVOS

Diseñar un prototipo de una red WAN de forma segura para Hardsoft mediante Red Privada Virtual (VPN) a través de Internet

OBJETIVOS ESPECIFICOS

- Realizar un estudio de la red actual de la empresa y a partir de la información obtenida, implementar la red local de Hardsoft
- Identificar, determinar y diseñar el direccionamiento, cableado y dispositivos necesarios que permitirán la conexión local y remota con las sucursales y usuarios externos.
- Conectar de forma segura las sucursales y empleados externos a los servidores y Bases de Datos de la sede central asegurando la confidencialidad de la información.
- Brindar privacidad a toda la información que está viajando a través de los túneles VPN, mediante la encriptación de los datos transmitidos, evitando el ingreso de terceros.
- Autenticación entre emisor y receptor para certificar que la comunicación sea efectuada directamente por los dos.

JUSTIFICACION

A medida que la empresa crece con el tiempo, requiere cambios drásticos que brinden seguridad, eficiencia, calidad y economía para satisfacer y mejorar las necesidades operativas que se presenta a diario; van a la mano las exigencias de las redes las cuales deben adaptarse a los cambios que se puedan presentar. Uno de estos cambios es optimizar las redes de área global a redes que tengan una distancia mayor a la local, permitiendo la conectividad de su personal y oficinas de otros edificios con la sede central y disponer de los mismos servicios sin importar su ubicación.

El diseño de una VPN para la empresa Hardsoft S.A es una forma económica en las comunicación entre oficinas, trabajadores externos, clientes, proveedores, mediante acceso remoto a los servidores, intranet y aplicativos de la empresa, reemplazando las costosas conexiones permanentes como Frame Relay, Punto a Punto o RDSI.
Hardsorf S.A estaría reduciendo costos en inversiones de hardware y servicios de telecomunicaciones costosas y proporcionales a la distancia implicada en la conexión de las oficinas. Con el uso de VPNs mediante Internet, la inversión en hardware es pequeña y la distancia no influiría en costos adicionales.

Otra ventaja al momento de implementar VPNs en Hardsoft S.A es incorporar o extender sus servicios como e-mail, streaming, gestión documental, VoIP a cualquier oficina o usuario externo, optimizando los recursos, mediante una clasificación y priorización de la información en función de su importancia. Por otro lado, esta tecnología brinda independencia en la selección de operador, por lo tanto puede cambiar de operador cuando lo desee sin necesidad de hacer cambio de equipos para adaptarse al otro operador.

El propósito es mostrar las ventajas que brinda una VPN en Hardsoft S.A, tales como la escalabilidad que tiene esta tecnología ya que puede adaptarse a mas usuarios y muchos más lugares a diferencia de las líneas dedicadas, la instalación de esta en cualquier PC Windows es muy sencilla, evita altos costos de actualizaciones y mantenimiento de las PC´s remotas, control de acceso según políticas de la empresa, ya que Hardsoft S.A podrá gozar de una conexión a una red con las características de una red privada.

1.2 MARCO METODOLOGICO

1.2.1 TITULO

IMPLEMENTACION DE LA RED PRIVADA VIRTUAL (VPN) A LAS SUCURSALES Y USUARIOS EXTERNOS DE LA EMPRESA HARDSOFT S.A

1.2.2 LINEA DE INVESTIGACION

El tema que se tratara en el trabajo Redes Privadas Virtuales está encaminado por la línea de investigación de Redes y telecomunicaciones, y se propone como objetivo emplear los medios necesarios para garantizar el adecuado funcionamiento de la red actual, permitiendo la comunicación remota con otros usuarios de forma económica y reduciendo los riesgos de pérdida y manipulación de la información, contribuyendo de esta manera al desarrollo tecnológico.

FORMULACION DEL PROBLEMA

- ¿Cuáles son los principales elementos para diseñar una red Privada Virtual (VPN) capaz de garantizar confidencialidad, seguridad, autenticación y autorización a la empresa Hardsoft S.A?

FORMULACION DE LA HIPOTESIS

Con la adecuación de una Red Privada Virtual en la empresa HardSoft S.A, se mejorara la comunicación y transmisión de datos de la sede principal con las sucursales de la empresa de forma segura y solucionando inconvenientes internos de conectividad.

RECOPILACION DE INFORMACION

Por medio de visitas a las sucursales de Hardsoft S.A se realizaran registros que permitan conocer y analizar cuantas sucursales se interconectar, cuantos equipos componen estas sedes, que tipos de aplicativos manejan en su intranet, como está compuesta la red LAN, con que tecnología de hardware y software disponen para implementar una VPN.

COMPROBACION DE LA HIPOTESIS

Mediante la simulación en Packet Tracer podremos divisar las conexiones LAN, WAN con las sucursales y el ISP, pruebas contra fallas, configuración de dispositivos de conexión y direccionamiento y tiempos de respuesta entre los equipos.

2. ANTECEDENTES

Anteriormente se había realizado un estudio superficial sobre las posibles alternativas que tenia la empresa para poderse comunicar con los usuarios externos (sucursales y empleados externos) en el momento de ampliar sus redes de área local a un espacio más amplio permitiendo la conectividad del personal y oficinas en otros edificios de forma segura, rápida y eficiente, que permitiera emplear los recursos con los que dispone la empresa, en este caso, comunicarse a través de internet haciendo uso de VPNs o Redes Privadas Virtuales.

Las redes corporativas se extienden de forma rápida, acomodándose a las necesidades de los empleados a larga distancia y oficinas remotas. Las VPNs son una solución económica de comunicación a nivel geográfico, es decir, acceso desde cualquier lugar del mundo a través de internet, siempre y cuando cuente con el usuario y contraseña asignada por la empresa; otra ventaja de emplear esta tecnología en la empresa Hardsoft S.A es la seguridad que se le brinda a la información manejada por el usuario remoto y las oficinas externas con el servidor principal de Hardsoft S.A.
Con la implementación de la VPN en Hardsoft S.A, se garantizara una mejora en la productividad de la empresa, genera oportunidades de comunicación adicionales, permitiendo otros medios para transferir, consultar o modificar datos importantes de la empresa brindando teletrabajo, igualmente se estaría reduciendo en gastos de telecomunicaciones en comparación con las conexiones permanentes o canales dedicados.

La VPN se basa en un protocolo de Túnel que cifra los datos que son transmitidos desde un lado de la VPN hacia el otro, es decir, los datos están cifrados desde el momento que entran a la VPN hasta que salen de ella y, por lo tanto, son incomprensibles para cualquiera que no se encuentre en uno de los extremos de la VPN, como si los datos viajaran a través de un túnel. En la VPN de dos equipos, el cliente de VPN es la parte que cifra y descifra los datos del lado del usuario y el servidor VPN o servidor de acceso remoto, es el elemento que descifra los datos del lado de la organización.
La principal tarea de esta proyectos es presentar un prototipo de diseño de una VPN a la empresa Hardsoft S.A y mostrarle las grandes ventajas que trae en su economía, productividad y desarrollo.

En la planeación de nuevas tecnologías para la ampliación de otras sucursales de la empresa, se analizara el propósito de la conexión, el alcance geográfico, los requisitos de tráfico y su infraestructura privada o pública dependiendo el caso y los recursos económicos con los que cuenta la empresa, con el objetivo de aumentar la rentabilidad, productividad de los empleados y reducción de costos de operación.

2.1 MARCO TEORICO

Red: [1]Es un conjunto de equipos y otros dispositivos, como impresoras, discos, entre otros, que se conectan entre sí con cables, para que puedan comunicarse entre ellos, con el fin de compartir información y recursos, haciendo que todas las personas o departamentos de una empresa, estén trabajando unidos, sin duplicar la información, transmitiéndola de forma rápida y eficaz.

Clasificación de las Redes

- **Por Alcance**

- **[2]Red de Área Local (LAN):** es una red que se limita a un área especial pequeña tal como un cuarto, un solo edificio o a un entorno de 200 metros, con repetidores podría llegar a la distancia de un campo de 1 kilómetro. Las redes de área local a veces se llaman una sola red de localización.
  Las redes de área local (local área networks) llevan mensajes a velocidades relativamente grandes entre computadores conectados a un único medio de comunicaciones: un cable de par trenzado. Un cable coaxial o una fibra óptica.

  Características

  - Tecnología broadcast (difusión) con el medio de transmisión compartido.
  - Capacidad de transmisión comprendida entre 1 Mbps y 1 Gbps.
  - Extensión máxima no superior a 3 km (una FDDI puede llegar a 200 km).
  - Uso de un medio de comunicación privado.
  - La simplicidad del medio de transmisión que utiliza (cable coaxial, cables telefónicos y fibra óptica).
  - La facilidad con que se pueden efectuar cambios en el hardware y el software.

- **Red de Área Metropolitana (MAN):** Es una red de alta velocidad (banda ancha) que da cobertura en un área geográfica extensa. las redes de área metropolitana (metropolitan area networks), se basan en el gran ancho de banda de las cableadas de cobre y fibra óptica recientemente instalados para la transmisión de videos, voz, y otro tipo de datos. Varias han sido las tecnologías utilizadas para implementar el encaminamiento en las redes LAN, desde Ethernet hasta ATM. IEEE ha publicado la especificación 802.6 [IEEE 1994], diseñado expresamente para satisfacer las necesidades de las redes

[1] PURSER, MICHAEL. Redes de Telecomunicación y Ordenadores. Ediciones Díaz de Santos S.A

[2] *www.unicrom.com/cmp_**red_lan**.asp*

WAN. la tecnología de pares de cobre se posiciona como la red más grande del mundo una excelente alternativa para la creación de redes metropolitanas, por su baja latencia (entre 1 y 50ms), gran estabilidad y la carencia de interferencias radioeléctricas, las redes MAN BUCLE, ofrecen velocidades de 10Mbps, 20Mbps, 45Mbps, 75Mbps, sobre pares de cobre y 100Mbps, 1Gbps y 10Gbps mediante Fibra Óptica.

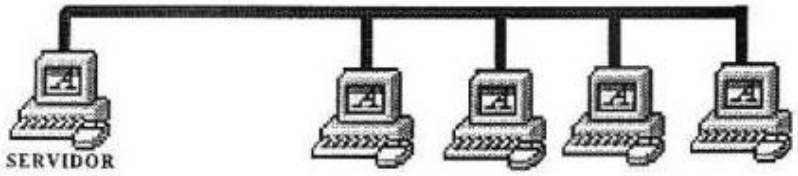
- **Red de Área Amplia (WAN):** Son redes informáticas que se extienden sobre un área geográfica extensa, estas pueden llevar mensajes entre nodos que están a menudo en diferentes organizaciones y quizás separadas por grandes distancias, pero a una velocidad menor que las redes LAN. El medio de comunicación esta compuesto por un conjunto de círculos de enlazadas mediante computadores dedicados, llamados rotures o encaminadores. Esto gestiona la red de comunicaciones y encaminan mensajes o paquetes hacia su destino.

Topologías Físicas

- **Topología de Bus:**

[3]Red cuya topología se caracteriza por tener un único canal de comunicaciones (denominado bus, troncal o backbone) al cual se conectan los diferentes dispositivos. De esta forma todos los dispositivos comparten el mismo canal para comunicarse entre sí.

Figura 1. Topología en Bus



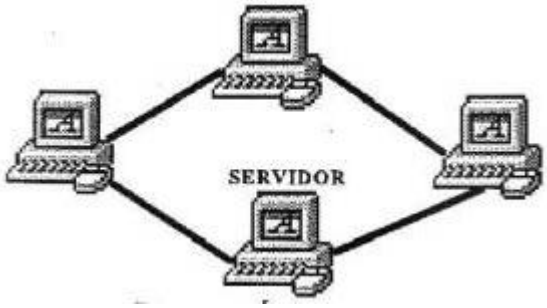
Fuente: http://platea.pntic.mec.es/~lmarti2/cableado.htm

- **Topología en Anillo:**

[3] TANENBAUM ANDREWS S. Redes de computadoras. Cuarta Edición. Página 16. Editorial Pearson Prentice Hall.

[4]En esta topología la estación está conectada a la siguiente y la última está conectada a la primera. Cada estación tiene un receptor y un transmisor que hace la función de repetidor, pasando la señal a la siguiente estación.

Figura 2 Topología en Anillo

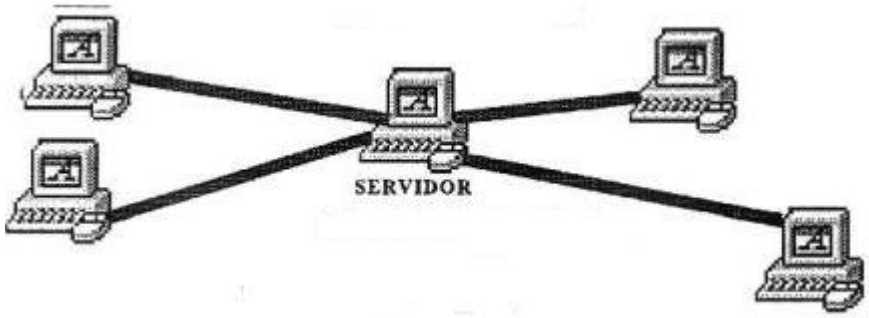


Fuente: http://platea.pntic.mec.es/~lmarti2/cableado.htm

- **Topología en Estrella:**

Es una red en la cual las estaciones están conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de éste.

Figura 3. Topología en Estrella



Fuente: http://platea.pntic.mec.es/~lmarti2/cableado.htm

- **Topología en Estrella Extendida:**

Es igual a la topología en estrella, con la diferencia de que cada nodo que se conecta con el nodo central también es el centro de otra estrella. Generalmente el

[4] http://es.wikipedia.org/wiki/Topologiaredes

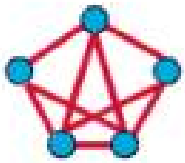
nodo central está ocupado por un hub o un switch, y los nodos secundarios por hubs. Esta conexión es utilizada actualmente por el sistema telefónico.
La ventaja de esto es que el cableado es más corto y limita la cantidad de dispositivos que se deben interconectar con cualquier nodo central.
La topología en estrella extendida es sumamente jerárquica, y busca que la información se mantenga local.

Figura 4. Topología en Estrella Extendida

- **Topología de Malla:**

Esta topología consiste en que cada nodo está conectado a uno o más de los otros nodos. De esta manera es posible llevar los mensajes de un nodo a otro por diferentes caminos. Si la red de malla está completamente conectada no puede existir absolutamente ninguna interrupción en las comunicaciones. Cada servidor tiene sus propias conexiones con todos los demás.

Figura 5. Topología en Malla



Estructura de la red LAN

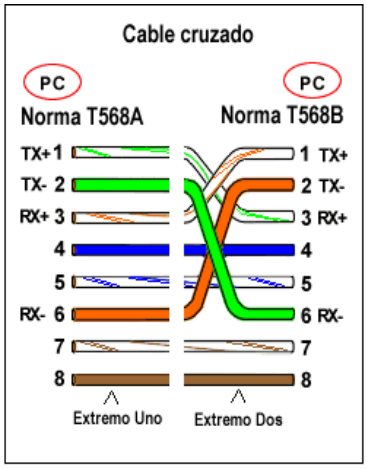
- **Cable Cruzado.**

[5]Es un cable que interconecta todas las señales de salida en un conector con las señales de entrada en el otro conector, y viceversa; permitiendo a dos dispositivos electrónicos conectarse entre sí con una comunicación full duplex.
El cable cruzado sirve para conectar dos dispositivos iguales, como 2 computadoras entre sí, para lo que se ordenan los colores de tal manera que no

[5] *windows.microsoft.com/.../Connect-two-computers-using-a-crossover-**cable***
PEREZ HERNANDEZ MARIA GABRIELA. Ciencias fundamentales y tecnología. Editorial Dikinson.

sea necesaria la presencia de un hub. Actualmente la mayoría de hubs o switches soportan cables cruzados para conectar entre sí.

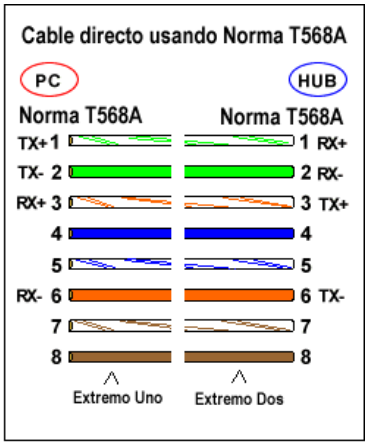
Figura 6. Normas Para conectar un Cable Cruzado



❖ Cable Directo

El cable directo de red sirve para conectar dispositivos diferentes, como un computador con un hub o switch. En este caso ambos extremos del cable deben tener la misma distribución. No existe diferencia alguna en la conectividad entre la distribución 568B y la distribución 568A siempre y cuando en ambos extremos se use la misma, en caso contrario hablamos de un cable cruzado.

Figura 7. Normas Para conectar un Cable Directo



Cableado de las Redes

La gran mayoría de las redes están conectadas por algún tipo de cableado, que actúa como medio de transmisión por donde pasan las señales entre los equipos. Hay disponibles una gran cantidad de tipos de cables para cubrir las necesidades y tamaños de las diferentes redes, desde las más pequeñas a las más grandes.

Tipos de Cableado

- Cable Coaxial.

Es relativamente barato, y era ligero, flexible y sencillo de manejar. Un cable coaxial consta de un núcleo de hilo de cobre rodeado por un aislante, un apantallamiento de metal trenzado y una cubierta externa.
El término apantallamiento hace referencia al trenzado o malla de metal (u otro material) que rodea algunos tipos de cable. El apantallamiento protege los datos transmitidos absorbiendo las señales electrónicas espúreas, llamadas ruido, de forma que no pasan por el cable y no distorsionan los datos.

El cable coaxial es más resistente a interferencias y atenuación que el cable de par trenzado. La malla de hilos protectora absorbe las señales electrónicas perdidas, de forma que no afecten a los datos que se envían a través del cable de cobre interno. Por esta razón, el cable coaxial es una buena opción para grandes distancias y para soportar de forma fiable grandes cantidades de datos con un equipamiento poco sofisticado.

Figura 8. Cable Coaxial

- Cable Par Trenzado

Un cable de par trenzado consta de dos hilos de cobre aislados y entrelazados. Hay dos tipos de cables de par trenzado: cable de par trenzado sin apantallar (UTP) y par trenzado apantallado (STP).

A menudo se agrupan una serie de hilos de par trenzado y se encierran en un revestimiento protector para formar un cable. El número total de pares que hay en un cable puede variar. El trenzado elimina el ruido eléctrico de los pares adyacentes y de otras fuentes como motores, relés y transformadores.

Cable de par trenzado sin apantallar (UTP)

El UTP, con la especificación 10BaseT, es el tipo más conocido de cable de par trenzado y ha sido el cableado LAN más utilizado en los últimos años. El segmento máximo de longitud de cable es de 100 metros.

El cable UTP tradicional consta de dos hilos de cobre aislados. Las especificaciones UTP dictan el número de entrelazados permitidos por pie de cable; el número de entrelazados depende del objetivo con el que se instale el cable.

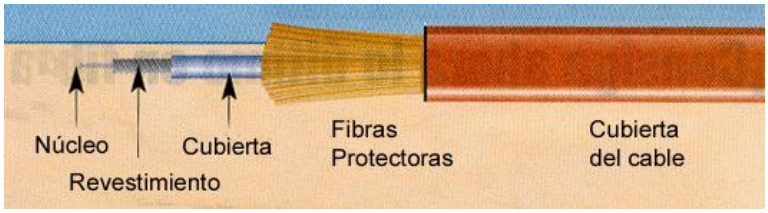
La especificación 568A Commercial Building Wiring Standard de la Asociación de Industrias Electrónicas e Industrias de la Telecomunicación (EIA/TIA) especifica el tipo de cable UTP que se va a utilizar en una gran variedad de situaciones y construcciones. El objetivo es asegurar la coherencia de los productos para los clientes. Estos estándares definen cinco categorías de UTP:

- **Categoría 1**. Hace referencia al cable telefónico UTP tradicional que resulta adecuado para transmitir voz, pero no datos. La mayoría de los cables telefónicos instalados antes de 1983 eran cables de Categoría 1.
- **Categoría 2**. Esta categoría certifica el cable UTP para transmisión de datos de hasta 4 megabits por segundo (mbps), Este cable consta de cuatro pares trenzados de hilo de cobre.
- **Categoría 3**. Esta categoría certifica el cable UTP para transmisión de datos de hasta 16 mbps. Este cable consta de cuatro pares trenzados de hilo de cobre con tres entrelazados por pie.
- **Categoría 4**. Esta categoría certifica el cable UTP para transmisión de datos de hasta 20 mbps. Este cable consta de cuatro pares trenzados de hilo de cobre.
- **Categoría 5**. Esta categoría certifica el cable UTP para transmisión de datos de hasta 100 mbps. Este cable consta de cuatro pares trenzados de hilo de cobre.
- **Categoría 5a**. También conocida como Categoría 5+ ó Cat5e. Ofrece mejores prestaciones que el estándar de Categoría 5. Para ello se deben cumplir especificaciones tales como una atenuación al ratio crosstalk (ARC) de 10 dB a 155 Mhz y 4 pares para la comprobación del Power Sum NEXT. Este estándar todavía no está aprobado
- **Nivel 7**. Proporciona al menos el doble de ancho de banda que la Categoría 5 y la capacidad de soportar Gigabit Ethernet a 100 m. El ARC mínimo de 10 dB debe alcanzarse a 200 Mhz y el cableado debe soportar pruebas de

Power Sum NEXT, más estrictas que las de los cables de Categoría 5 Avanzada.

- **Categoría 5**. La TIA/EIA 568A especifica solamente las Categorías para los cables de pares trenzados sin apantallar (UTP). Cada una se basa en la capacidad del cable para soportar prestaciones máximas y mínimas. Hasta hace poco, la Categoría 5 era el grado superior especificado por el estándar TIA/EIA. Se definió para ser capaz de soportar velocidades de red de hasta 100 Mbps en transmisiones de voz/datos a frecuencias de hasta100 MHz. Las designaciones de Categoría están determinadas por las prestaciones UTP. El cable de Categoría 5 a100 MHz, debe tener el NEXT de 32 dB/304,8 mts. y una gama de atenuación de 67dB/304,8 mts, Para cumplir con el estándar, los cables deben cumplir solamente las mínimos estipulados, Con cable de Categoría 5 debidamente instalado, podrá esperar alcanzar las máximas prestaciones, las cuales, de acuerdo con los estándares, alcanzarán la máxima velocidad de traspaso de Mbps,
- **Categoría 5a**. La principal diferencia entre la Categoría 5 (568A) y Categoría 5a (568A-5) es que algunas de las especificaciones han sido realizadas de forma más estricta en la versión más avanzada. Ambas trabajan a frecuencias de 100 MHz. Pero la Categoría 5e cumple las siguientes especificaciones: NEXT: 35 dB; PS-NEXT: 32 dB, ELFEXT: 23.8 dB; PS-ELFEXT: 20.8 dB, Pérdida por Retorno: 20.1 dB, y Retardo: 45 ns, Con estas mejoras, podrá tener transmisiones Ethernet con 4 pares, sin problemas, full-duplex, sobre cable UTP. En el futuro, la mayoría de las instalaciones requerirán cableado de Categoría 5e así como sus componentes.
- **Categoría 6 y posteriores**. Ahora ya puede obtener un cableado de Categoría 6, aunque el estándar no ha sido todavía creado. Pero los equipos de trabajo que realizan los estándares están trabajando en ello. La Categoría 6 espera soportar frecuencias de 250 MHz, dos veces y media más que la Categoría 5. En un futuro cercano, la TIA/EIA está estudiando el estándar para la Categoría 7, para un ancho de banda de hasta 600 MHz. La Categoría 7, usará un nuevo y aún no determinado tipo de conector.
- **Cable de fibra óptica:** En el cable de fibra óptica las señales que se transportan son señales digitales de datos en forma de pulsos modulados de luz. Esta es una forma relativamente segura de enviar datos debido a que, a diferencia de los cables de cobre que llevan los datos en forma de señales electrónicas, los cables de fibra óptica transportan impulsos no eléctricos. Esto significa que el cable de fibra óptica no se puede pinchar y sus datos no se pueden robar. El cable de fibra óptica es apropiado para transmitir datos a velocidades muy altas y con grandes capacidades debido a la carencia de atenuación de la señal y a su pureza.

Figura 9. Cable Fibra Óptica



El cable de fibra óptica se utiliza si necesita transmitir datos a velocidades muy altas y a grandes distancias en un medio muy seguro.
El cable de fibra óptica no se utiliza si tiene un presupuesto limitado, no tiene el suficiente conocimiento para instalar y conectar los dispositivos de forma apropiada o El precio del cable de fibra óptica es competitivo con el precio del cable de cobre alto de gama. Cada vez se hace más sencilla la utilización del cable de fibra óptica, y las técnicas de pulido y terminación requieren menos conocimientos que hace unos años.

MODELO OSI (Open System Interconnection)

[6]El Modelo de Referencia de Interconexión de Sistemas Abiertos, conocido mundialmente como Modelo OSI (Open System Interconnection), fue creado por la ISO (Organización Estándar Internacional) y en él pueden modelarse o referenciarse diversos dispositivos que reglamenta la ITU (Unión de Telecomunicación Internacional), con el fin de poner orden entre todos los sistemas y componentes requeridos en la transmisión de datos, además de simplificar la interrelación entre fabricantes. Así, todo dispositivo de cómputo y telecomunicaciones podrá ser referenciado al modelo y por ende concebido como parte de unos sistemas interdependiente con características muy precisas en cada nivel.

Nivel de Aplicación

Es el nivel más cercano al usuario y a diferencia de los demás niveles, por ser el más alto o el último, no proporciona un servicio a ningún otro nivel. En OSI el nivel de aplicación se refiere a las aplicaciones de red que vamos a utilizar para transportar las aplicaciones del usuario.

[6]CNAMS,Theme=ccna3theme,Style=ccna3,Language=es,Version=1,RootID=knet-lcms_exploration1_es_40,Engine=static/CHAPID=null/RLOID=null/RIOID=null/theme/cheetah.html?cid=0600000000&l1=tl&l2=en&chapter=1

FTP (File Transfer Protocol), Mail, Rlogin, Telnet, son entre otras las aplicaciones incluidas en el nivel 7 del modelo OSI y sólo cobran vida al momento de requerir una comunicación entre dos entidades. En Resumen se puede decir que la capa de Aplicación se dice que es una sesión específica de aplicación (API), es decir, son los programas que ve el usuario.

Nivel de Presentación

Se refiere a la forma en que los datos son representados en una computadora. Proporciona conversión de códigos y reformateo de datos de la aplicación del usuario. Es sabido que la información es procesada en forma binaria y en este nivel se llevan a cabo las adaptaciones necesarias para que pueda ser presentada de una manera más accesible.
La capa de Presentación es aquella que provee representación de datos, es decir, mantener la integridad y valor de los datos independientemente de la representación

Nivel de Sesión

Este nivel es el encargado de proveer servicios de conexión entre las aplicaciones, tales como iniciar, mantener y finalizar una sesión. Establece, mantiene, sincroniza y administra el diálogo entre aplicaciones remotas.
La capa de Sesión es un espacio en tiempo que se asigna al acceder al sistema por medio de un login en el cual obtenemos acceso a los recursos del mismo servidor conocido como "circuitos virtuales”. La información que utiliza nodos intermedios que puede seguir una trayectoria no lineal se conoce como "sin conexión".

Nivel de Transporte

En este nivel se realiza y se garantiza la calidad de la comunicación, ya que asegura la integridad de los datos. Es aquí donde se realizan las retransmisiones cuando la información fue corrompida o porque alguna trama (del nivel 2) detectó errores en el formato y se requiere volver a enviar el paquete o datagrama.
Los protocolos TCP (Transmission Control Protocol) y UDP (User Datagram Protocol) son característicos del nivel del transporte del modelo OSI, al igual que SPX (Sequenced Packet Exchange) de Novell.
La capa de Transporte es la integridad de datos de extremo a extremo o sea que se encarga el flujo de datos del transmisor al receptor verificando la integridad de los mismos por medio de algoritmos de detección y corrección de errores, la capa de Red es la encargada de la información de enrutador e interceptores y aquella que maneja el Hardware (HW), ruteadores, puentes, multiplexores para mejorar el enrutamiento de los paquetes.

Enlace de Datos

Conocido también como nivel de Trama (Frame) o Marco, es el encargado de preparar la información codificada en forma binaria en formatos previamente definidos por el protocolo a utilizar.
Tiene su aplicación en el contexto de redes WAN y LAN ya que como se estableció previamente la transmisión de datos no es mas que el envió en forma ordenada de bits de información. En el nivel de enlace de datos se lleva a cabo el direccionamiento físico de la información; es decir, se leerán los encabezados que definen las direcciones de los nodos (para el caso WAN) o de los segmentos (para el caso LAN) por donde viajarán las tramas.
La capa de Enlace de Datos es aquella que transmite la información como grupos de bits, o sea que transforma los bits en frame o paquetes por lo cual si recibimos se espera en conjunto de señales para convertirlos en caracteres en cambio si se manda se convierte directamente cada carácter en señales ya sean digitales o analógicos.

Nivel Físico

Es el primer nivel del modelo OSI y en él se definen y reglamentan todas las características físicas-mecánicas y eléctricas que debe cumplir el sistema para poder operar. Como es el nivel más bajo, es el que se va a encargar de las comunicaciones físicas entre dispositivos y de cuidar su correcta operación. Es bien sabido que la información computarizada es procesada y transmitida en forma digital siendo esta de bits: 1 y 0.
La capa Físico transmite el flujo de bits sobre un medio físico y aquella que representa el cableado, las tarjetas y las señales de los dispositivos.

VPN: Red privada virtual, [7]es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

VPN de acceso remoto

Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autentificados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

[7] http://www.configurarequipos.com/doc499.html

VPN punto a punto

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicional, sobre todo en las comunicaciones internacionales.

TUNNELING

[8]La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo una PDU determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser SSH.

PDU

Unidades de Datos de Protocolo. Se utiliza para el intercambio entre unidades parejas, dentro de una capa del modelo OSI. Existen dos clases de PDUs:

- PDU de datos, que contiene los datos del usuario final (en el caso de la capa de aplicación) o la PDU del nivel inmediatamente superior.

- PDU de control, que sirven para gobernar el comportamiento completo del protocolo en sus funciones de establecimiento y ruptura de la conexión, control de flujo, control de errores, etc. No contienen información alguna proveniente del nivel N+1.

Cada capa del modelo OSI en el origen debe comunicarse con capa igual en el lugar destino. Esta forma de comunicación se conoce como comunicación de par-a-par.

Durante este proceso, cada protocolo de capa intercambia información en lo que se conoce como unidades de datos de protocolo (PDU), entre capas iguales. Cada

[8] http://beta.redes-linux.com/manuales/vpn/Estudio_VPN.pdf

capa de comunicación, en el computador origen, se comunica con un PDU específico de capa y con su capa igual en el computador destino.

IPsec

(Abreviatura de **Internet Protocol security**) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

PPTP

Point to Point Tunneling Protocol, [9]es un protocolo desarrollado para implementar redes privadas virtuales o VPN. Point-To-Point Tunneling Protocol (PPTP) permite el seguro intercambio de datos de un cliente a un servidor formando una Red Privada Virtual (VPN por el anglicismo Virtual Private Network), basado en una red de trabajo vía TCP/IP. El punto fuerte del PPTP es su habilidad para proveer en la demanda, multi-protocolo soporte existiendo una infraestructura de área de trabajo, como INTERNET. Esta habilidad permitirá a una compañía usar Internet para establecer una red privada virtual (VPN) sin el gasto de una línea alquilada.

Esta tecnología que hace posible el PPTP es una extensión del acceso remoto del PPP (point-to-point-protocol. La tecnología PPTP encapsula los paquetes ppp en Communications, 3com / Primary Access, ECI Telematics y US Robotics. Datagramas IP para su transmisión bajo redes basadas en TCP/IP. PPTP y VPN: El Protocolo Point-To-Point Tunneling Protocol viene incluido con WindowsNT 4.0 Server y Workstation. Los PC's que tienen corriendo dentro de ellos este protocolo pueden usarlo para conectar con toda seguridad a una red privada como un cliente de acceso remoto usando una red pública como Internet.

Una característica importante en el uso del PPTP es su soporte para VPN. La mejor parte de esta característica es que soporta VPNs sobre public-switched telephone networks (PSTNs) que son los comúnmente llamados accesos telefónicos a redes.

Usando PPTP una compañía puede reducir en un gran porcentaje el coste de distribución de una red extensa, la solución del acceso remoto para usuarios en continuo desplazamiento porque proporciona seguridad y comunicaciones cifradas sobre estructuras de área de trabajo existentes como PSTNs o Internet.

[9] **ESTUDIO SOBRE LAS VPN (REDES PRIVADAS VIRTUALES) 4º INGENIERÍA INFORMÁTICA.. VALADOLID. UNIVERSIDAD DE ALLLADOLID.. Mª Nieves Gutiérrez González, Ana Rosa Sancho Buzón Y Amadeo Casas Cuadrado**

L2TP

(*Layer 2 Tunneling Protocol*) fue diseñado por un grupo de trabajo de IETF como el heredero aparente de los protocolos PPTP y L2F, creado para corregir las deficiencias de estos protocolos y establecerse como un estándar aprobado por el IETF (RFC 2661). L2TP utiliza PPP para proporcionar acceso telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado. L2TP define su propio protocolo de establecimiento de túneles, basado en L2F. El transporte de L2TP está definido para una gran variedad de tipos de paquete, incluyendo X.25, Frame Relay y ATM.

Al utilizar PPP para el establecimiento telefónico de enlaces, L2TP incluye los mecanismos de autenticación de PPP, PAP y CHAP. De forma similar a PPTP, soporta la utilización de estos protocolos de autenticación, como RADIUS.

A pesar de que L2TP ofrece un acceso económico, con soporte multiprotocolo y acceso a redes de área local remotas, no presenta unas características criptográficas especialmente robustas. Por ejemplo:

- Sólo se realiza la operación de autenticación entre los puntos finales del túnel, pero no para cada uno de los paquetes que viajan por él. Esto puede dar lugar a suplantaciones de identidad en algún punto interior al túnel.
- Sin comprobación de la integridad de cada paquete, sería posible realizar un ataque de denegación del servicio por medio de mensajes falsos de control que den por acabado el túnel L2TP o la conexión PPP subyacente.
- L2TP no cifra en principio el tráfico de datos de usuario, lo cual puede dar problemas cuando sea importante mantener la confidencialidad de los datos.
- A pesar de que la información contenida en los paquetes PPP puede ser cifrada, este protocolo no dispone de mecanismos para generación automática de claves, o refresco automático de claves. Esto puede hacer que alguien que escuche en la red y descubra una única clave tenga acceso a todos los datos transmitidos.

A causa de estos inconvenientes, el grupo del IETF que trabaja en el desarrollo de PPP consideró la forma de solventarlos. Ante la opción de crear un nuevo conjunto de protocolos para L2TP del mismo estilo de los que se están realizando para IPSec, y dado la duplicación del trabajo respecto al propio grupo de desarrollo de IPSec que supondría, se tomó la decisión de utilizar los propios protocolos IPSec para proteger los datos que viajan por un túnel L2TP.

L2TP es en realidad una variación de un protocolo de encapsulamiento IP. Un túnel L2TP se crea encapsulando una trama L2TP en un paquete UDP, el cual es encapsulado a su vez en un paquete IP, cuyas direcciones de origen y destino definen los extremos del túnel. Siendo el protocolo de encapsulamiento más externo IP, los protocolos IPSec pueden ser utilizados sobre este paquete, protegiendo así la información que se transporta por el túnel.

RADIUS

Remote **A**uthentication **D**ial-**I**n **U**ser **S**erver. Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1813 UDP para establecer sus conexiones. Cuando se realiza la conexión con un ISP mediante módem, DSL, cable módem, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo NAS (Servidor de Acceso a la Red o Network Access Server (NAS)) *sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS. El servidor* RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etc.

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.

RADIUS fue desarrollado originalmente por Livingston Enterprises para la serie PortMaster de sus Servidores de Acceso a la Red(NAS), más tarde se publicó como RFC 2138 y RFC 2139. Actualmente existen muchos servidores RADIUS, tanto comerciales como de código abierto. Las prestaciones pueden variar, pero la mayoría pueden gestionar los usuarios en archivos de texto, servidores LDAP, bases de datos varias, etc. Los servidores Proxy RADIUS se utilizan para una administración centralizada y pueden reescribir paquetes RADIUS al vuelo (por razones de seguridad, o hacer conversiones entre dialectos de diferentes fabricantes).

3. INGENIERIA DEL PROYECTO

3.2 PLANEACION INGENIERIL

Hardsoft S.A desea comunicar todas sus sucursales y usuarios externos mediante una red de recursos de carácter público, manteniendo el mismo sistema de gestión y mismas políticas de acceso que se usan en las redes privadas.
Para la implementación de la Red Privada Virtual (VPN) tendremos en cuenta la estructura de la red LAN en cada una de las sucursales de la empresa, es decir, cuantos equipos estarán conectados, que protocolos se implementaran para la comunicación y seguridad de la información, dispositivos empleados, direccionamiento y cableado. Con base a la información obtenida, se realizaran unos ajustes a la red LAN de cada sucursal si lo necesitara y se configurara la Red Privada Virtual en los equipos locales y remotos.

Análisis de Requerimientos

La empresa ha decidido ampliar y unificar su red privada más allá de su área geográfica, empleando una red pública como internet, reduciendo los costos frente a las conexiones WAN y obteniendo las mismas ventajas en seguridad, productividad y oportunidades de comunicación adicionales.
Con el fin de recopilar, analizar y verificar las necesidades del cliente, se tendrá en cuenta el manejo de las funciones que el sistema será capaz de realizar y las limitantes que se pueden presentar en la implementación tales como fiabilidad, rendimiento, mantenimiento, portabilidad, entre otras.

Los requerimientos que se tendrán en cuenta para la especificación del sistema y el modelo de análisis son los siguientes:

- Identificar los Skateholders:

Las personas involucradas en el desarrollo del sistema son:

- Sucursales
- Usuarios Internos
- Usuarios Externos
- Red LAN
- Red VPN

- Identificar los requerimientos:

Requerimientos Funcionales

Red LAN:

- Determinar cuántos equipos estarán conectados en cada sucursal mediante la recopilación de información, con el fin de realizar el direccionamiento IP a cada subred de Hardsoft, permitiendo que cada equipo sea identificado dentro de la red.
- Establecer los dispositivos (switch, router, tarjetas Ethernet), cableado (conector RJ45, Cable par trenzado) a utilizar en la red.
- Configurar las tarjetas de red de cada uno de los equipos de las sucursales, teniendo en cuenta el direccionamiento IP de cada subred.

Red VPN

- Identificación de usuarios, es decir, que la VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a los no autorizados mediante el Servidor VPN que realiza la autenticación de acceso.
- Establecer una dirección del cliente en la red Privada y que esta se conserve
- Encriptar los datos a través de túneles VPN para que no puedan ser leídos
- Generar y renovar claves para el cliente y el Servidor.
- Conexión de las sedes y los usuarios Remotos, mediante una conexión permanente a internet y una dirección IP fija, la cual usaran los usuarios remotos para conectarse a la VPN.
- Intercambio de información en tiempo real y disponibilidad de esta sin importar la ubicación del usuario.
- Conexión del servidor a través del router que estará conectado al ISP continuamente y la configuración del protocolo VPN que se utilizara para la conexión.
- Interconexión total a la red de todos los usuarios tanto internos como externos de forma segura a través de una infraestructura pública.
- Flexibilidad y facilidad de uso en el ingreso remoto a los aplicativos de la empresa.

Requerimientos No Funcionales

- La Red LAN y VPN deben funcionar en los Sistemas Operativos XP y Vista, ya que los equipos de la empresa cuenta con Windows.
- Los usuarios deben ser capaces de utilizar todas las funciones de la red VPN, tras un entrenamiento que se le dará los empleados.
- El sistema controlara la validez y coherencia de los datos ingresados en la conexión VPN

Resultados del Análisis

Actualmente la empresa se está comunicando mediante correo electrónico y llamadas telefónicas para mantenerse informada una sede de la otra sobre las ventas, actualización de mercancía, entre otras tareas, lo cual hace que los datos no se efectúen en tiempo real, generando retrasos en las respuestas a los clientes y procesos internos de la empresa. Con el fin de evitar estos medios de comunicación, se pensó en una reestructuración total en el modo de acceder a los datos, mediante la creación de una red que interconecta tanto la red LAN como la WAN con la posibilidad de tener un acceso total a los equipos y aplicativos independientemente del lugar donde se encuentre.

Hardsoft S.A cuenta con 40 empleados, ubicados en las distintas sedes y departamentos que conforman la empresa, a cada uno de ellos se le asigno un computador con las siguientes características:

- Sistema Operativo XP y Vista
- Paquete Office.
- Cuentas en Outlook para los empleados.
- Aplicativos Internos de la empresa (Software para el manejo de inventarios, Contabilidad, Ventas). Instalados exclusivamente en los equipos que lo requieran.
- Otros Software (Navegador, Java, Fhash Player, Acrobet, Real Player, etc).

Por petición del Gerente, los computadores de los empleados tendrán acceso limitado a internet, es decir, no podrán ingresar a Redes Sociales (Facebook, Twitter, Hi5, etc), paginas de ocio, entretenimiento entre otras. El servicio de internet se empleara principalmente para revisar correos y la intranet.
Las sedes de Hardsoft S.A. se conectaran al ISP por medio de ADSL o Línea de Abonado Digital Asimétrica, esta tecnología transmite la información con un ancho de banda sobre líneas normales de teléfono, sin interferir en las llamadas telefónicas.
Las especificaciones mencionadas anteriormente también se tendrán en cuenta para los usuarios remotos (empleados de Hardsoft.

Con base a la formulación y recopilación de información obtenida al principio del proyecto se obtuvo la siguiente información sobre estructura física de las sedes que funcionaran en Hardsoft:

Tabla 4. Distribución de las áreas de la Sede Lago

AREA	Número Host
Gerencia	4
Recursos Humanos	3
Sistemas	3
Contabilidad	2
Ventas	4
Bodega	2
TOTAL	18

Tabla 5. Distribución de las áreas de la Sede Centro

AREA	Número Host
Administración	2
Sistemas	2
Ventas	4
Bodega	2
TOTAL	10

Tabla 6. Distribución de las áreas de la Sede Galerías

AREA	Número Host
Administración	2
Sistemas	2
Ventas	4
Bodega	2
TOTAL	10

Análisis de Riesgos

Al implementar la Red Privada Virtual (VPN) se debe detectar las vulnerabilidades que se pueden presentar a nivel de seguridad, la cual debe proporcionar como mínimo la autenticación del usuario y restringir el acceso a los usuarios no autorizados. Si no se contara con ese requerimiento, cualquier persona malintencionada podría conectarse a los recursos e información de la red local.

Un factor importante a tener en cuenta es la red local (LAN), ya que a partir del buen funcionamiento y adecuada distribución de esta, se puede lograr un balance de cargas entre los usuarios internos como externos, de lo contrario podrían generarse colisiones de paquetes y por ende perdida de la información, generando problemas de interconectividad tanto en la red LAN como WAN.

Al momento de conectar las redes LAN de las sucursales y los usuarios remotos, se debe implementar el mismo protocolo para evitar incompatibilidad en la conexión o comunicación en el envió y recepción de los mensajes; otros factores que se tendrán en cuenta y que generarían fallos a la red son la configuración inadecuada de los servidores o la mala elección del cableado estructurado generando demoras e interferencias en la transmisión de los datos.

Una vez identificados los puntos vulnerables para la implementación de la Red Privada Virtual en Hardsoft, se tendrán en cuenta y se trabajara principalmente en ellos para evitar inconsistencias en la red. Como la VPN emplea una infraestructura pública, se emplearan un sistema de encriptación y autenticación mediante túneles virtuales entre las sedes, asegurando la confidencialidad e integridad de los datos transmitidos a través de internet, también se tendrá el protocolo de túnel de VPN a implementar en la red, el cual debe ser compatible con la configuración WAN y LAN.

3.2 Diseño Ingenieril

Hardsoft S.A se compone de 7 áreas Gerencia, Recursos Humanos, Sistemas, Contabilidad, Ventas y Bodega, las cuales están distribuidas en tres sitios estratégicos Lago, Centro y Galerías. La Sede del Lago es la Principal, en esta sede se administraran las redes Ethernet, WIFI, protocolos, y servidores que proveerán los datos solicitados por las otras sucursales.

A continuación se mencionaran los servidores que Hardsoft utilizara:

- Servidor DNS: Traducción de la dirección IP de un servidor Web a nombres de dominio y viceversa.
- Servidor WEB: Permitirá el control de acceso a los empleados tanto internos como a usuarios externos.
- Servidor FTP: Brinda los servicios de archivos ya sea en la red LAN de Hardsoft S.A o a los empleados remotos.
- Servidor Correo: Permite la administración de las cuentas de correo de los empleados de Hardsoft S.A.
- Servidor Radius: Permite la autenticación y autorización para aplicaciones de acceso a la red mediante DSL, modem, cable modem, Ethernet o WI-FI.

Estos servidores serán consultados por las sucursales y los empleados remotos.

Las sucursales Centro, Galerías y empleados remotos se comunicaran con la Sede Principal Lago mediante la Red Privada Virtual, utilizando un esquema cliente-servidor.
Para el direccionamiento de las subredes de las sucursales se utilizara una IP clase C, en la red LAN el direccionamiento comienza a partir de la IP 192.168.1.0 y para los enlaces WAN se empleara una dirección fija que nos brinde el proveedor de servicios en este caso es la 200.200.1.0.

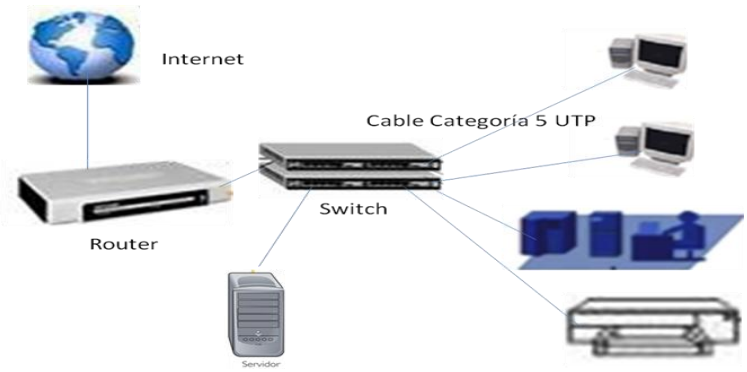
3.2.1. Configuración LAN de las Sucursales de Hardsoft

Para la conexión de la red de área local de la empresa, se emplearan dos arquitecturas de red:

- **La tecnología Ethernet** también conocido como estándar IEEE 802.3, el cual se basa en que *todos los equipo en una red Ethernet están conectados a la misma línea de comunicación compuesta por cables cilíndricos*. Con esta arquitectura se tendrá en cuenta el cableado, infraestructura física y direccionamiento local de cada una de las sucursales de Hardsoft S.A.

  Los equipos de cada sucursal de Hardsoft S.A están conectados a la misma línea de transmisión y comunicación local, la cual emplea un protocolo denominado CSMA/CD (Carrier Sense Multiple Access with Collision Detect); con este protocolo cualquier equipo está autorizado a transmitir a través de la línea en cualquier momento y sin ninguna prioridad entre ellos, permitiendo que cada equipo verifica que no haya ninguna comunicación en la línea antes de transmitir, por ejemplo, si dos equipos estuvieran transmitiendo simultáneamente se produciría una colisión por lo tanto los equipos interrumpen su comunicación y esperan un periodo de tiempo aleatorio, luego una vez que el primero ha excedido el período de tiempo, puede volver a transmitir.

Figura 10. Tecnología Ethernet



- **Tecnología WIFI** o especificación IEEE 802.11 (ISO/IEC 8802-11), es un estándar internacional que define las características de la red de Área Local Inalámbrica (WLAN). Con base en esta tecnología se tendrá en cuenta las características de señalización para la transmisión de datos.
  Hardsoft empleara tanto la red Ethernet como la red WiFi para empleados que requieran de una oficina móvil local que permita al igual que la tecnología Ethernet transmitir y recibir datos, compartir periféricos, acceso a un servidor de correo, navegar a través de internet, etc, a velocidades de 11 Mbps o incluso superiores sin que afecte la rapidez de las aplicaciones; y finalmente para los clientes que deseen adquirir un equipo o dispositivo con tarjeta de red inalámbrica, este medio le permitirá al usuario hacer pruebas y verificar que el producto que se le está vendiendo funciona adecuadamente.

Figura 11. Tecnología WIFI

3.2.2. Estructura de la Red LAN

Las redes Ethernet empleadas para la conexión local se realizaran mediante la interfaz física RJ45 que transmite información a través de un cable doble par trenzado (UTP Categoría 5) abreviatura 100Base-TX con velocidad de 100 Mb/sg, la estructura de este cable se efectuara según las normas EIA/TIA-568A (T568A) y la EIA/TIA-568B (T568B) dependiendo del tipo de dispositivo se vaya a conectar.

- **Cable de red cruzada para dispositivos Iguales**

El cable cruzado es utilizado para conectar dos dispositivos directamente o equipos activos entre si, como hub con hub, con switch, router, etc.

El cable es ponchado de un extremo del cable con la norma T568A y el otro extremo con la norma T568B**.**

- **Cable de red Directa para dispositivos Diferentes**

Este tipo de cable es utilizado para conectar computadores a equipos activos de red, como Hubs, Switchers, Routers. El cable es ponchado con ambos extremos iguales, es decir, que si se utilizo la norma T568A en un extremo del cable, en el otro extremo también se debe aplicar la misma norma T568A.

3.2.2.1 Estructura LAN de las Sedes

Se realizara un diseño de las redes de las sedes de Hardsoft para establecer la normatividad del cableado dependiendo de los dispositivos a conectar, también se establecerá el direccionamiento LAN y WAN, configuración de los equipos e implementación de la VPN.

Con base a la información obtenida al comienzo del proyecto sobre la cantidad de equipos necesarios para cada sede, se realizara la división de las subredes a partir de la Dirección de red 192.168.1.0 comenzando por la sede que cuenta con más equipos permitiendo así una mayor organización.

El diseño LAN se realizo de la siguiente manera:

La sede Lago estará conformadas por seis áreas administrativas: Gerencia, Recursos Humanos, Sistemas, Contabilidad, Ventas, Bodega, Las sedes Centro y Galerías contaran con los departamentos de administración, sistemas, ventas y bodega y ambas serán sucursales de la Sede Lago de Hardsoft.

La sede Lago será la principal de Hardsoft, y en ella se manejara toda la parte administrativa.

El diseño de la red de esta y el resto de las sedes se tendrá en cuenta la escalabilidad para que la red local pueda expandir y admitir nuevos usuarios y aplicaciones sin que se afecte el rendimiento del servicio. Cada host conectado debe contar con una dirección IP para poderse identificar y localizar dentro o fuera de la red y así lograr un punto de conexión.
Los host de las Sedes tendrán una dirección IP lógica única que identificara la ubicación ya sea en la red local o una diferente. La dirección IP es conocida comúnmente como notación decimal y se conforma de 32 bits divididos por dos partes: Número de Red y Número de Host o Nodo.
El numero de Red identifica un único segmento de red dentro de un conjunto de redes TCP/IP más grande y el numero de host identifica un nodo TCP/IP dentro de cada red lo cual identificara de forma exclusiva un único sistema en su propia red.

Teniendo en cuenta lo mencionado anteriormente, podremos determinar que la Sede Lago tendrá un segmento de red conformado por 18 host, las Sedes Centro y Galerías también contaran con un segmento de red pero con menor cantidad de host con un total de 10, en las tres subredes se tendrá en cuenta los usuarios a futuro para no limitar la red local de cada uno de ellos. El tipo de clase que se empleara será la clase C, la cual permite máximo 254 host y es suficiente para los 38 host de la red de Hardsoft.

La red será simulada a través de Packet Tracer, la cual nos permitirá configurar los dispositivos, realizar pruebas de conectividad, implementar protocolos de comunicación, entre otras actividades, de forma real. Una limitante del programa es que no se puede configurar totalmente las redes VPN ya que no cuenta con algunas funciones para la ejecución.

Figura 12. Diseño General de Red Hardsoft.

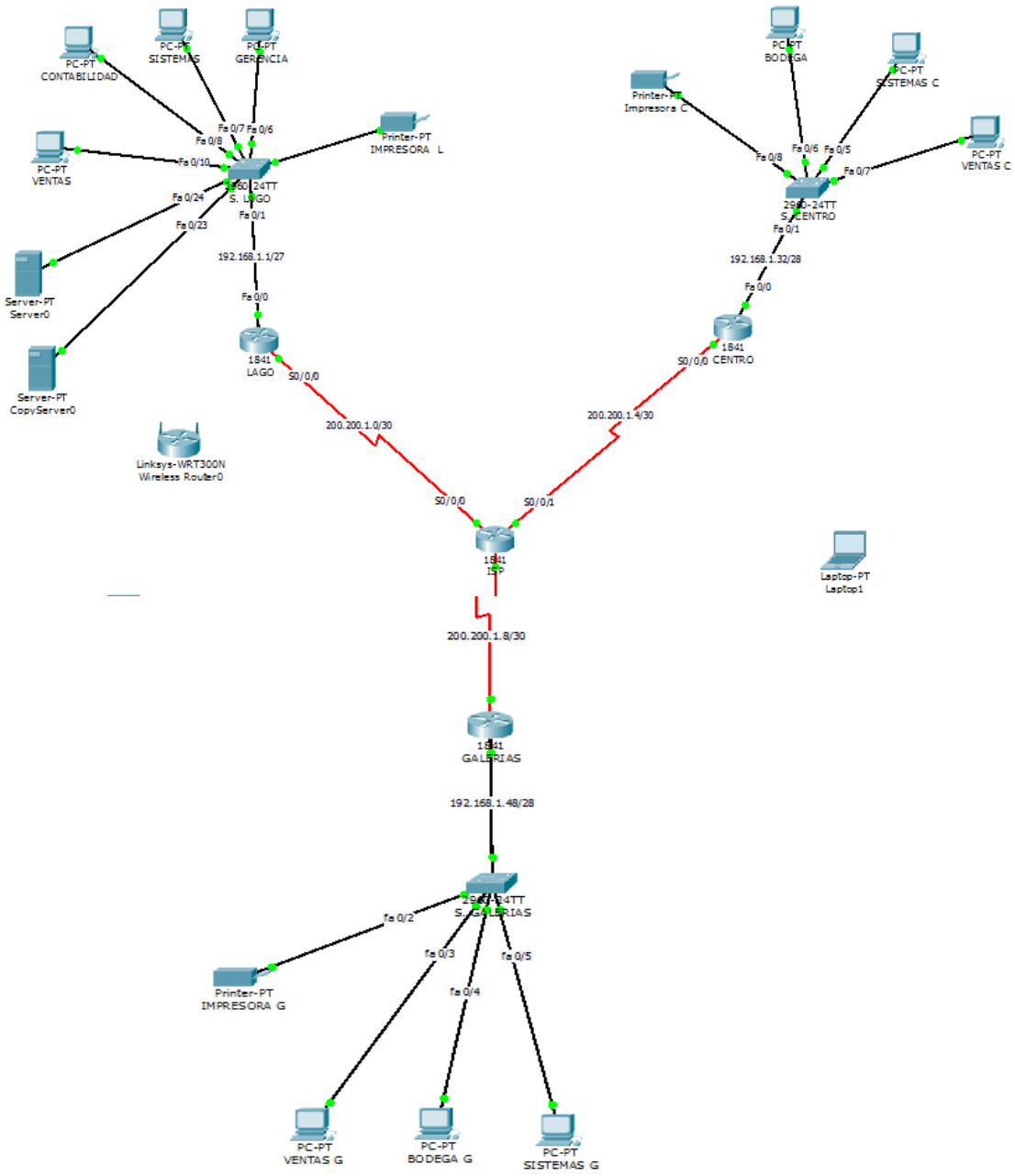


Tabla 7. **Direccionamiento Red General.**

DIRECCIONAMIENTO LAN											
ID	DIR. RED	BROADCAST	VSLM	MASCARA	UTILIZABLES	USADOS	AMPLIABLES	1° VALIDA	ULT. VALIDA	GATEWAY	DESCRIPCION
1	192.168.1.0	192.168.1.31	27	255.255.255.224	30	18	12	192.168.1.1	192.168.1.30	192.168.1.1	LAN 1 ADM LAGO
2	192.168.1.32	192.168.1.47	28	255.255.255.240	14	10	4	192.168.1.33	192.168.1.46	192.168.1.33	LAN 2 ADM CENTRO
3	192.168.1.48	192.168.1.63	28	255.255.255.240	14	10	4	192.168.1.49	192.168.1.62	192.168.1.49	LAN 3 ADM GALERIAS
ENLACES WAN											
1	200.200.200.0	200.200.200.3	3	255.255.255.252	2	2	0	200.200.200.1	200.200.200.2	N.A	WAN ISP - LAGO
2	200.200.200.4	200.200.200.7	3	255.255.255.252	2	2	0	200.200.200.5	200.200.200.6	N.A	WAN ISP - CENTRO
3	200.200.200.8	200.200.200.11	3	255.255.255.252	2	2	0	200.200.200.9	200.200.200.10	N.A	WAN ISP - GALERIAS

- **Sede Lago**

La sede Lago está conformada por dos pisos en el primero se encuentra ubicado ventas, y bodga con un total de 6 host, en el segundo se encuentra los servidores ubicados un cuarto de red donde se administraran tanto la red local como las de las dos sucursales y el Proveedor de Servicios de Internet (ISP), el departamento de administración, sistemas y contabilidad conformado por 12 host como se muestra en el esquema: (Ver figura 13).

Figura 13. Estructura Física de la Sede Lago a Internet

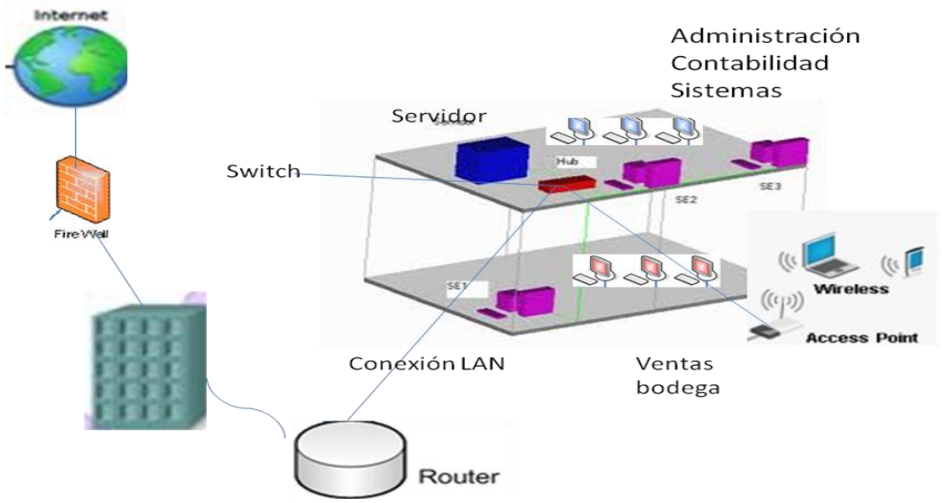
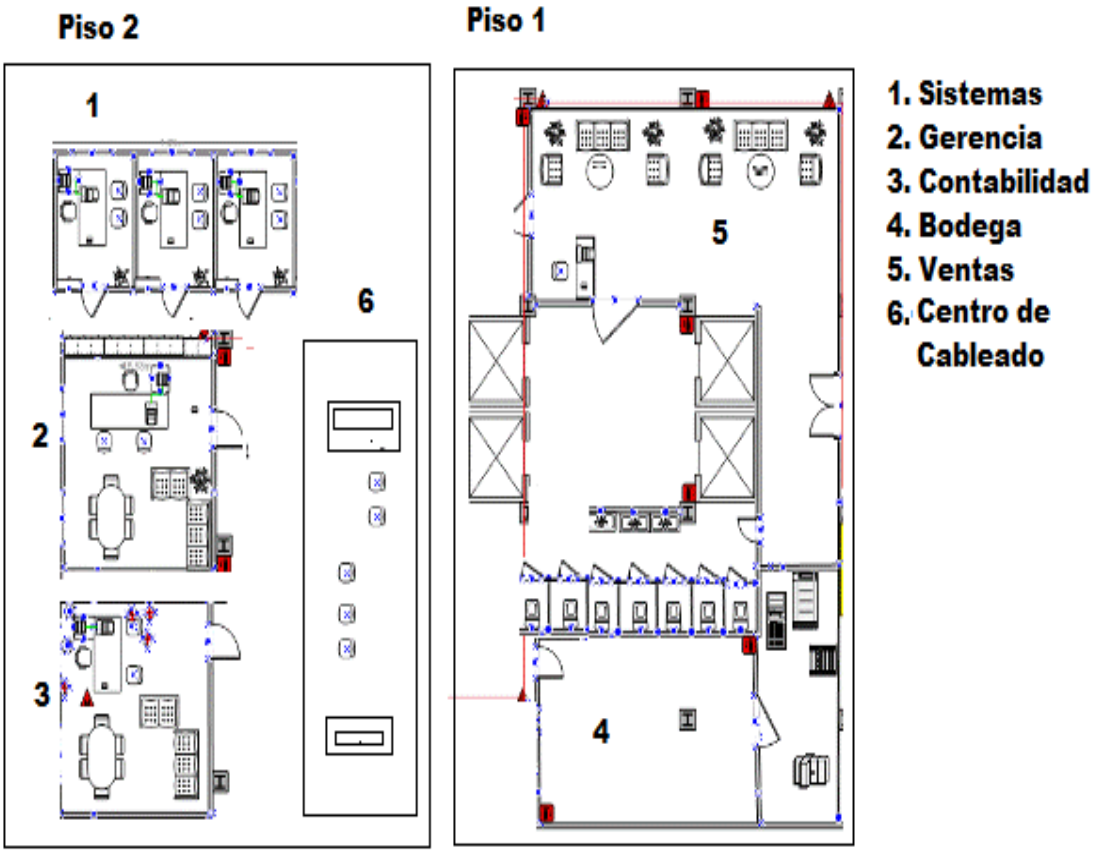


Figura 14. Plano de la sede Lago de Hardsoft



El diseño de red de la Sede Lago, se encuentra un router LAGO, enlazado al Proveedor de Servicios ISP y a la red LAN. La red LAN corresponde la estructura física, en ella encontramos un switch llamado S LAGO que está conectado directamente al router LAGO, por medio de un cable directo es decir con sus dos extremos iguales. Este Switch está conectado finalmente a los host de los usuarios finales, como equipos, servidores e impresoras, por cables directos. Cada uno de estos dispositivos están configurados con una dirección IP partiendo de la 192.168.1.0 con máscara de subred /27 o 255.255.255.192. La simulación de la red la realizaremos a través de packet tracer como se muestra en la siguiente figura:

Figura 15. Diseño Red LAN Sede Lago en Packet Tracer

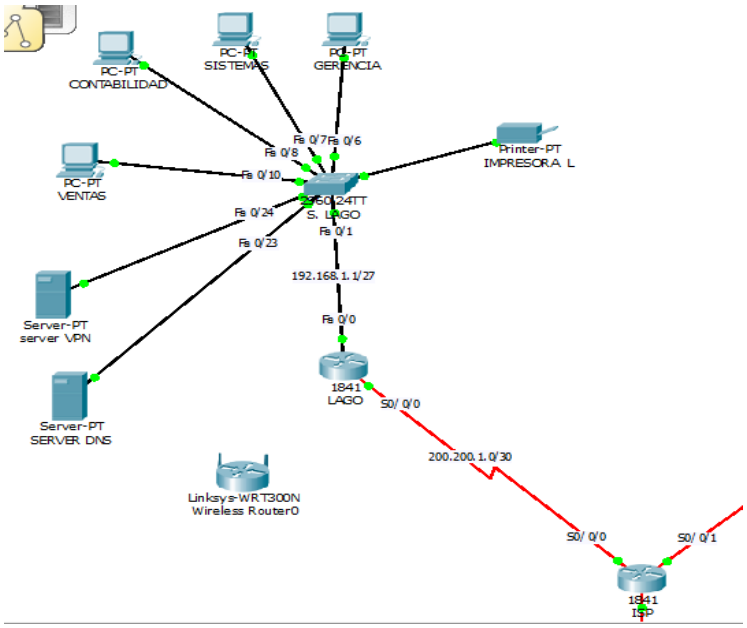


Tabla 8. Direccionamiento Sede Lago

Dispositivo	Interfaz	Dirección IP	Mascara Subred	Gateway
R Lago-SLago	Fa 0/0	192.168.1.1	255.255.255.224	N.A
R Lago – ISP	Fa 0/1	200.200.1.2	255.255.255.224	N.A
S Lago	Fa 0/1	192.168.1.3	255.255.255.224	192.168.1.1
PC1 Gerencia	Fa 0/6	192.168.1.5	255.255.255.224	192.168.1.1
PC2 Sistemas	Fa 0/7	192.168.1.9	255.255.255.224	192.168.1.1
PC3 Ventas	Fa 0/8	192.168.1.13	255.255.255.224	192.168.1.1
PC4 Contabil,	Fa 0/10	192.168.1.17	255.255.255.224	192.168.1.1
PC5 Bodega	Fa 0/12	192.168.1.20	255.255.255.224	192.168.1.1
Impresora LG	Fa 0/9	192.168.1.23	255.255.255.224	192.168.1.1
Servidor VPN	Fa 0/23	192.168.1.29	255.255.255.224	192.168.1.1

- **Sede Centro**

La sede Centro está conformada por un solo piso donde está ubicada la administración de esa sede, sistemas, ventas, y bodega. La sede se comunica con la sede principal (Sede Lago) para mantener al tanto sobre los movimientos que se efectúan en ella, al igual adquirir información sobre los cambios que se han realizado durante el día. La estructura física se mostrara a continuación.

Figura 16. Estructura Física de la Sede Centro

El diseño de red de la Sede Centro, se encuentra un router CENTRO, enlazado al Proveedor de Servicios ISP y a la red LAN. La red LAN encontramos un switch llamado S CENTRO que está conectado directamente al router CENTRO, por medio de un cable directo. Este Switch está conectado finalmente a los host de los usuarios finales, como equipos, servidores e impresoras, por cables directos. Cada uno de estos dispositivos están configurados con una dirección IP partiendo de la 192.168.1.33 con máscara de subred /28 o 255.255.255.240

Figura 17. **Plano de la sede Centro de Hardsoft**

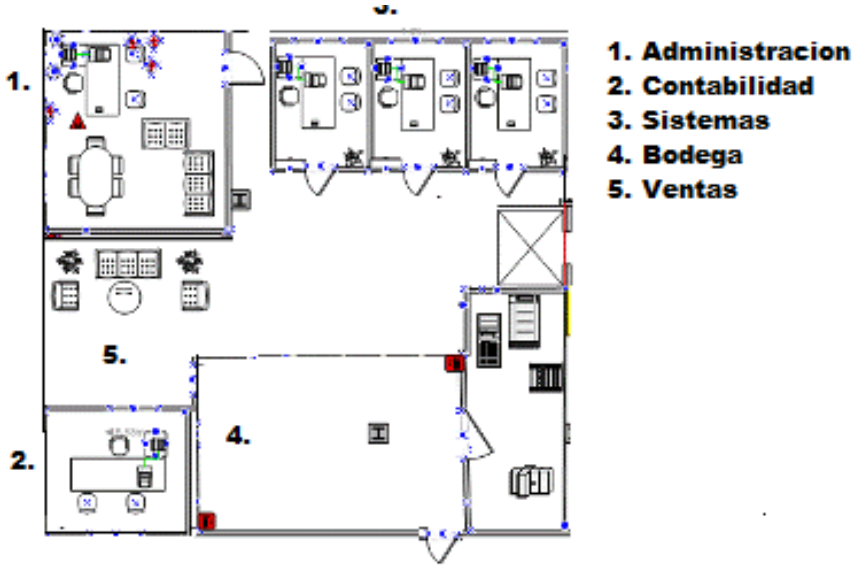


Figura 18. Diseño Red LAN Sede Centro en Packet Tracer

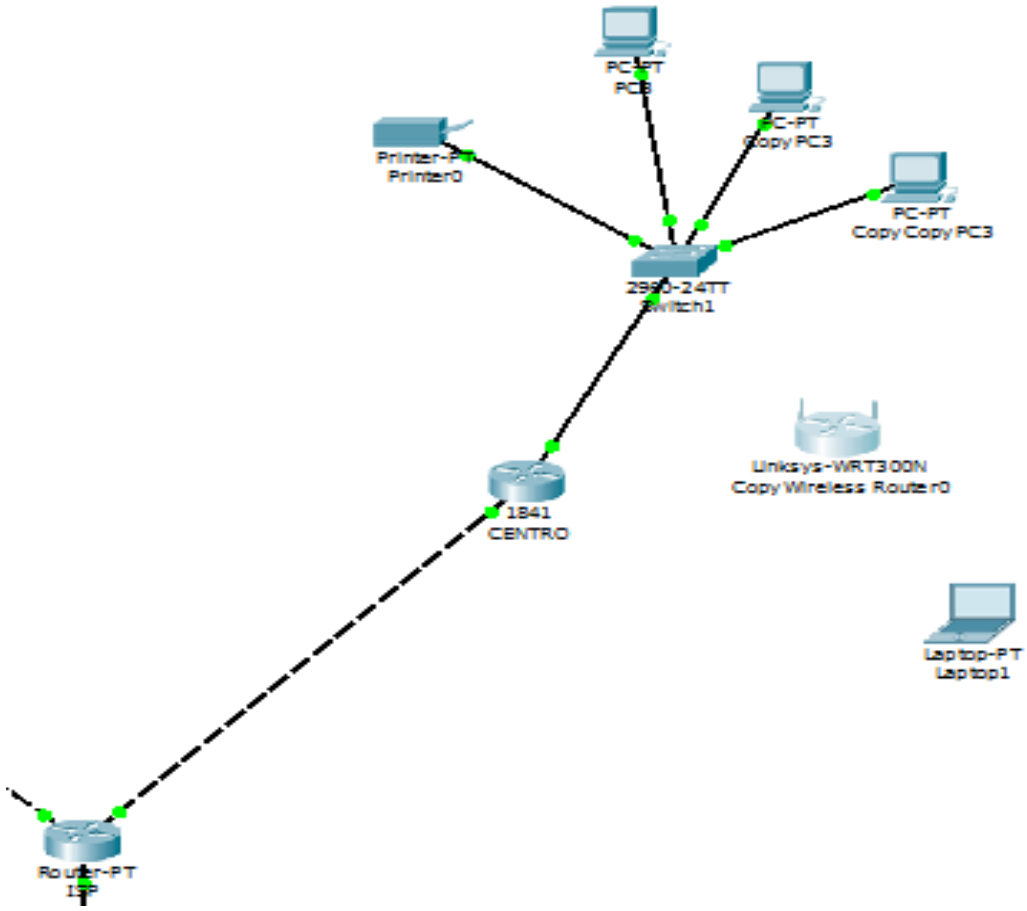


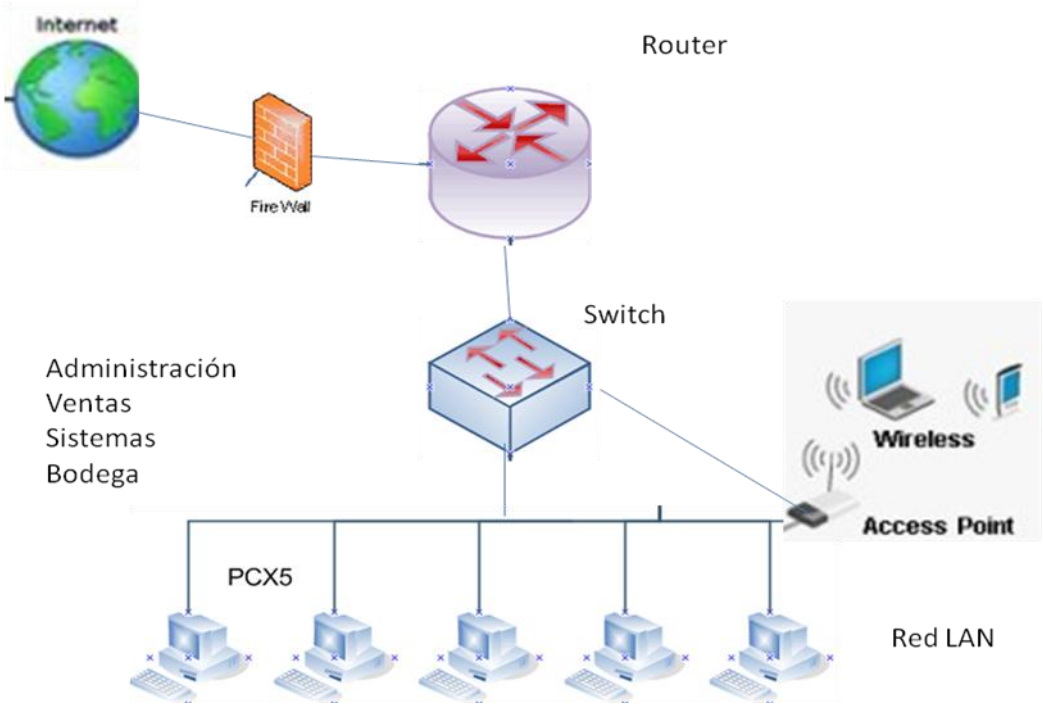
Tabla 9. Direccionamiento Sede Centro

Dispositivo	Interfaz	Dirección IP	Mascara Subred	Gateway
R Centro-SCentro	Fa 0/0	192.168.1.33	255.255.255.240	N.A
R Centro – ISP	Fa 0/1	200.200.1.6	255.255.255.252	N.A
S Centro	Fa 0/1	192.168.1.35	255.255.255.240	192.168.1.33
PC1 Admin	Fa 0/6	192.168.1.38	255.255.255.240	192.168.1.33
PC2 Sistemas	Fa 0/7	192.168.1.40	255.255.255.240	192.168.1.33
PC3 Ventas	Fa 0/8	192.168.1.42	255.255.255.240	192.168.1.33
PC5 Bodega	Fa 0/12	192.168.1.44	255.255.255.240	192.168.1.33
Impresora CT	Fa 0/9	192.168.1.37	255.255.255.240	192.168.1.33

❖ **Sede Galerías**

La sede Galerías al igual que la sede Centro se encuentra establecida en un solo piso donde está ubicada la administración de esa sede, sistemas, ventas, y bodega. Esta sede también mantiene conexión con la sede principal (Sede Lago) para mantener al tanto sobre los movimientos que se efectúan en ella, al igual adquirir información sobre los cambios que se han realizado durante el día, intercambiar información, etc. La estructura física se mostrara a continuación:

Figura 19. Estructura Física de la Sede Galerías



El diseño de red de la Sede Galería, se encuentra un router GALERIA, enlazado al Proveedor de Servicios ISP y a la red LAN. La red LAN encontramos un switch llamado S GALERIA que está conectado directamente al router GALERIA, por medio de un cable directo. Este Switch está conectado finalmente a los host de los usuarios finales, como equipos, servidores e impresoras, por cables directos. Cada uno de estos dispositivos están configurados con una dirección IP partiendo de la 192.168.1.48 con máscara de subred /28 o 255.255.255.240

Figura 20. Plano de la Sede Galerías

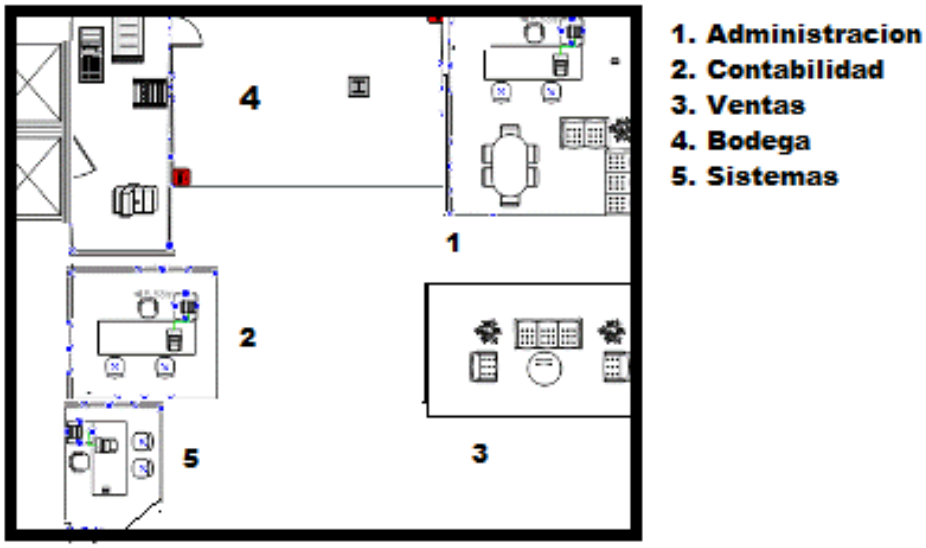


Figura 21. Diseño Red LAN Sede Galerías

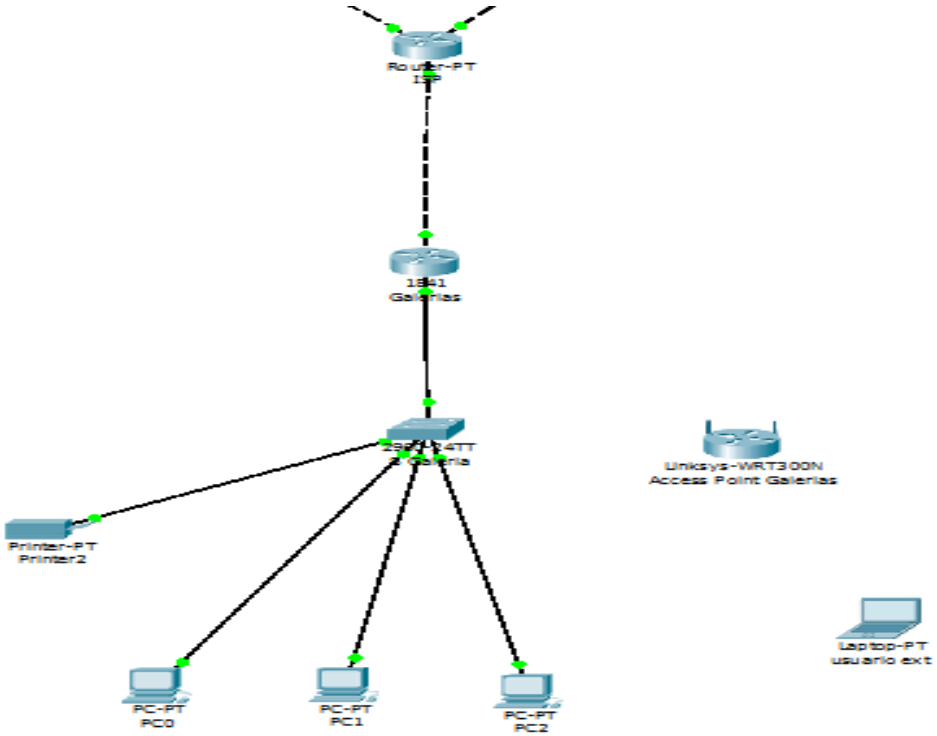


Tabla 10. Direccionamiento Sede Galerías

Dispositivo	Interfaz	Dirección IP	Mascara Subred	Gateway
RGalerías-SGaleria	Fa 0/0	192.168.1.49	255.255.255.240	N.A
R Galerías – ISP	Fa 0/1	200.200.1.9	255.255.255.252	N.A
S Centro	Fa 0/1	192.168.1.51	255.255.255.240	192.168.1.49
PC1 Admin	Fa 0/6	192.168.1.52	255.255.255.240	192.168.1.49
PC2 Sistemas	Fa 0/7	192.168.1.54	255.255.255.240	192.168.1.49
PC3 Ventas	Fa 0/8	192.168.1.57	255.255.255.240	192.168.1.49
PC5 Bodega	Fa 0/12	192.168.1.59	255.255.255.240	192.168.1.49
Impresora CT	Fa 0/9	192.168.1.61	255.255.255.240	192.168.1.49

Para la red WAN se contratara los servicios de un proveedor de comunicaciones el cual nos asigno la dirección 200.200.1.0, estos enlaces serán conexiones ADSL (***A****symmetric* ***D****igital* ***S****ubscriber* ***L****ine*), del proveedor al cliente que en este caso es las sedes de Hardsoft; esta tecnología de acceso a internet, consiste en una transmisión de datos analógica a través de un par simétrico de cobre que lleva la línea telefónica permitiendo velocidades superiores que permiten la transmisión de voz y datos que serán divididos por un splitter o filtro. La distribución para el direccionamiento IP de la Red WAN es la siguiente para cada sede:

Tabla 11. Direccionamiento WAN de Hardsoft.

WAN	MASCARA	1RA VALIDA	ULTIM.VALIDA	BROADCAST
200.200.1.0	255.255.255.252/30	200.200.1.1	200.200.1.2	200.200.1.3
200.200.1.4	255.255.255.252/30	200.200.1.5	200.200.1.6	200.200.1.7
200.200.1.8	255.255.255.252/30	200.200.1.9	200.200.1.10	200.200.1.11

Una vez estructuradas las conexiones LAN y WAN en todas las sucursales de Hardsoft, se configuraran las VPNs a los equipos de cada sucursal y usuarios remotos:

3.3 CONFIGURACION DE LA VPN (Red Privada Virtual)

En la configuración de la VPN (Red Privada Virtual) se debe contar con:

- Conexión a internet rápida tanto para el servidor como para los equipos locales y remotos.
- Una Dirección IP para los recursos a compartir.
- Una dirección IP para el servidor.

- El firewall debe estar inactivo en todos los PC que se van a conectar.

❖ **Elementos Principales de la Configuración de una Red con VPN**

- Hardsoft utiliza tres redes privadas: la sede Lago 192.168.1.0 con máscara de subred 255.255.255.192, sede Centro 192.168.1.32 mascara de subred 255.255.255.240 y sede Cedritos 192.168.1.48 mascara de subred 255.255.255.240.
- La dirección IP WAN en Internet asignado por el Proveedor de Servicios de Internet (ISP) de Hardsoft S.A para las sucursales con conexión ADSL, el direccionamiento de la Sede Lago es la 200.200.1.1, Sede Centro 200.200.1.5 y Sede Cedrito 200.200.1.9.
- El servidor VPN que estará ubicado en la Sede Principal Lago, el cual proporciona el enrutamiento de paquetes hacia ubicaciones en intranet o Internet

Hardsoft S.A desea comunicar sus sedes sin invertir demasiado dinero en infraestructura como se ha mencionado anteriormente, por lo tanto se quiere realizar una convergencia del modelo actual de la red a la implementación de una tecnología que no requiera conexiones costosas y que sea confiable, estable y segura, además que garantice la calidad de los servicios de voz, video y datos sin que estos sean afectados entre si.

Actualmente las redes de Hardsoft cuentan con la configuración LAN en cada una de sus sedes como se mostro anteriormente en este trabajo, pero el objetivo a lograr es permitir la comunicación de las sedes sin necesidad de emplear canales dedicados, empleando la tecnología VPN. La siguiente figura muestra como funciona la Red Privada Virtual sobre un canal público “internet y reemplazando los canales dedicados por un protocolo de túnel, el cual cifra los datos que se transmiten desde un lado de la VPN a otra, impidiendo que la información sea comprensible cualquiera que no se encuentre en los extremos de las VPNs.

Basada en la estructura LAN que se adecuo en cada una de las sucursales, la tecnología VPN se podrá acomodar a cada requerimiento de acceso con las que se cuente, permitiendo una migración fácil de administrar y mantener.

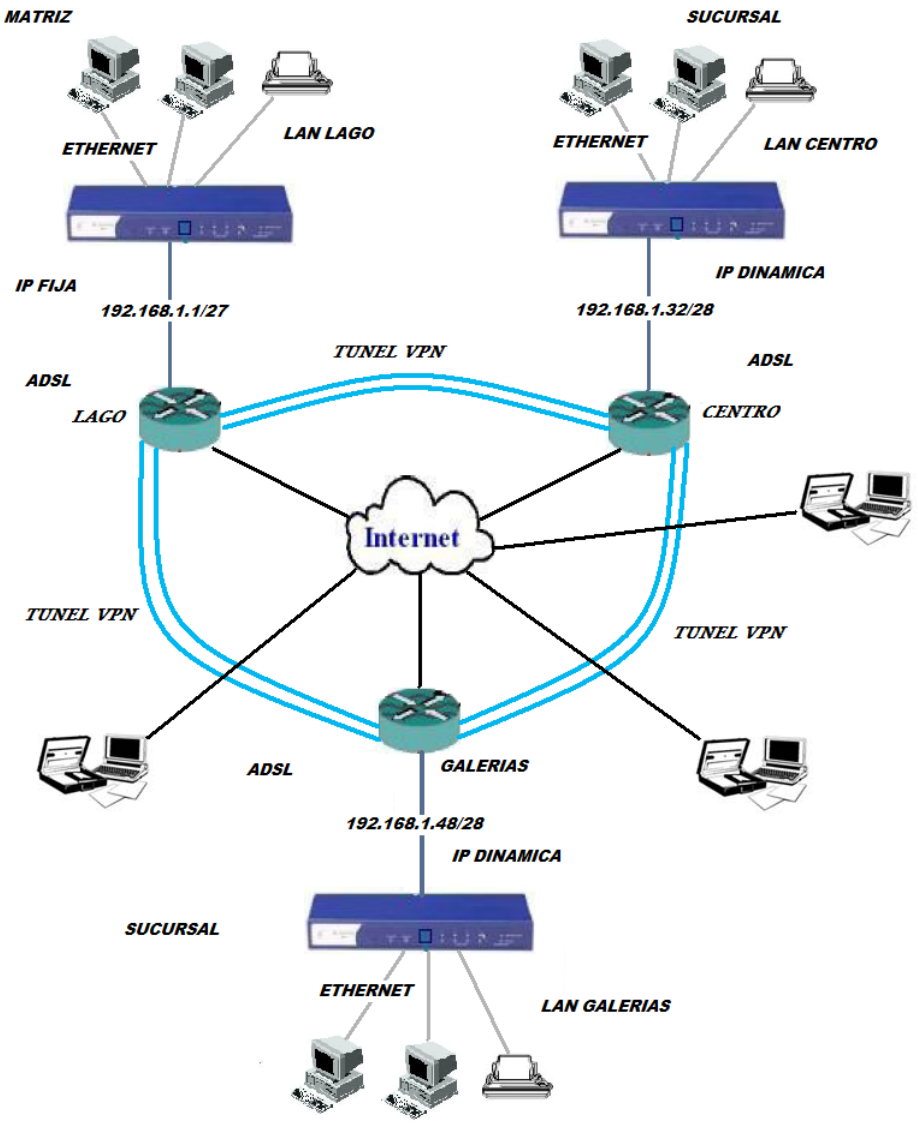
Direccionamiento del Servidor VPN

Para la configuración del servidor VPN y el Cliente VPN, utilizaremos el siguiente direccionamiento en las Tarjetas de Red Ethernet del Servidor y el PC del cliente

Tabla 12. Direccionamiento IP del Servidor VPN

DIRECCIONAMIENTO CON EL SERVIDOR				
DIR. RED	**DIR. IP**	**MASCARA**	**GATEWAY**	**DESCRIPCION**
192.168.1.0	192.168.1.27	255.255.255.224	192.168.1.1	Servidor VPN
192.168.1.0	192.168.1.15	255.255.255.224	192.168.1.27	Cliente VPN

Figura 22 Esquema de Red VPN



3.3.1 Configuración de la VPN en el Servidor de Hardsoft S.A

Con la Red Privada Virtual (VPN), los datos se encapsulan o se envuelven con un encabezado que proporciona información de enrutamiento, lo que permite que los datos atraviesen la red compartida o pública hasta llegar a su punto de destino, de esta forma, los datos se cifran para conservar la confidencialidad, por lo tanto, los paquetes interceptados en la red compartida o pública no se pueden descifrar sin las claves de cifrado**.**
Para la configuración de una conexión entrante en un servidor de acceso remoto, hay que habilitar el puerto a través del que los clientes se van a conectar al servidor este tema lo abordaremos más adelante.

En la configuración del Servidor VPN tenemos dos opciones:

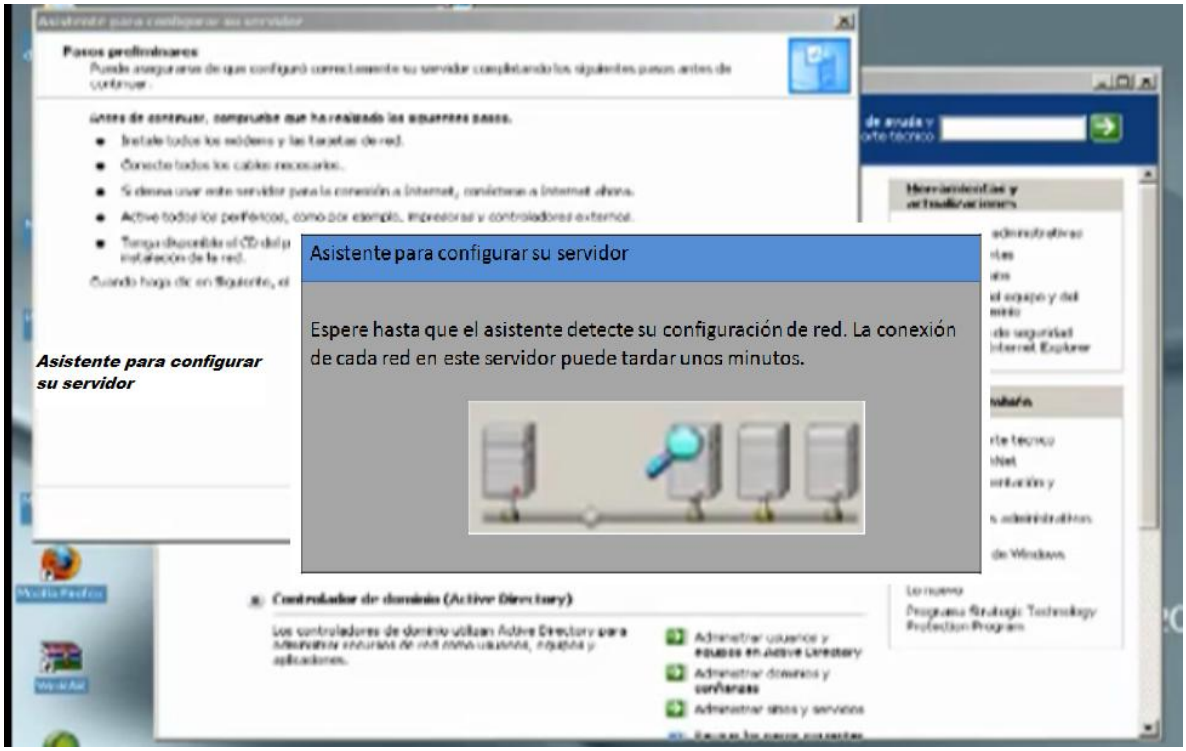
Si el equipo no es servidor ni miembro de un dominio, las conexiones entrantes se configuran en Windows con el Asistente para conexión de red que se utiliza para las conexiones salientes.
Si el equipo es servidor y miembro de un dominio, para configurar conexiones entrantes las realizaremos mediante Server 2003 a través de herramientas Enrutamiento y acceso remoto. El uso de esta herramienta puede ayudar a configurar redes privadas virtuales y conjuntos de módems en un servidor de acceso remoto.

Por medio del servidor VPN los equipos remotos podrán interactuar con la Red LAN como si estuvieran dentro de esta, este servidor será la puerta de enlace para comunicar los usuarios remotos con los locales. A continuación mostramos como configurar el Servidor VPN:

1. Para la configuración del servidor VPN, primero debemos habilitarlo. Vamos a inicio y click en Administrar su Servidor. En la ventana Administra su Servidor damos doble click a Agregar o Quitar Función. Aparece un asistente y le damos siguiente.

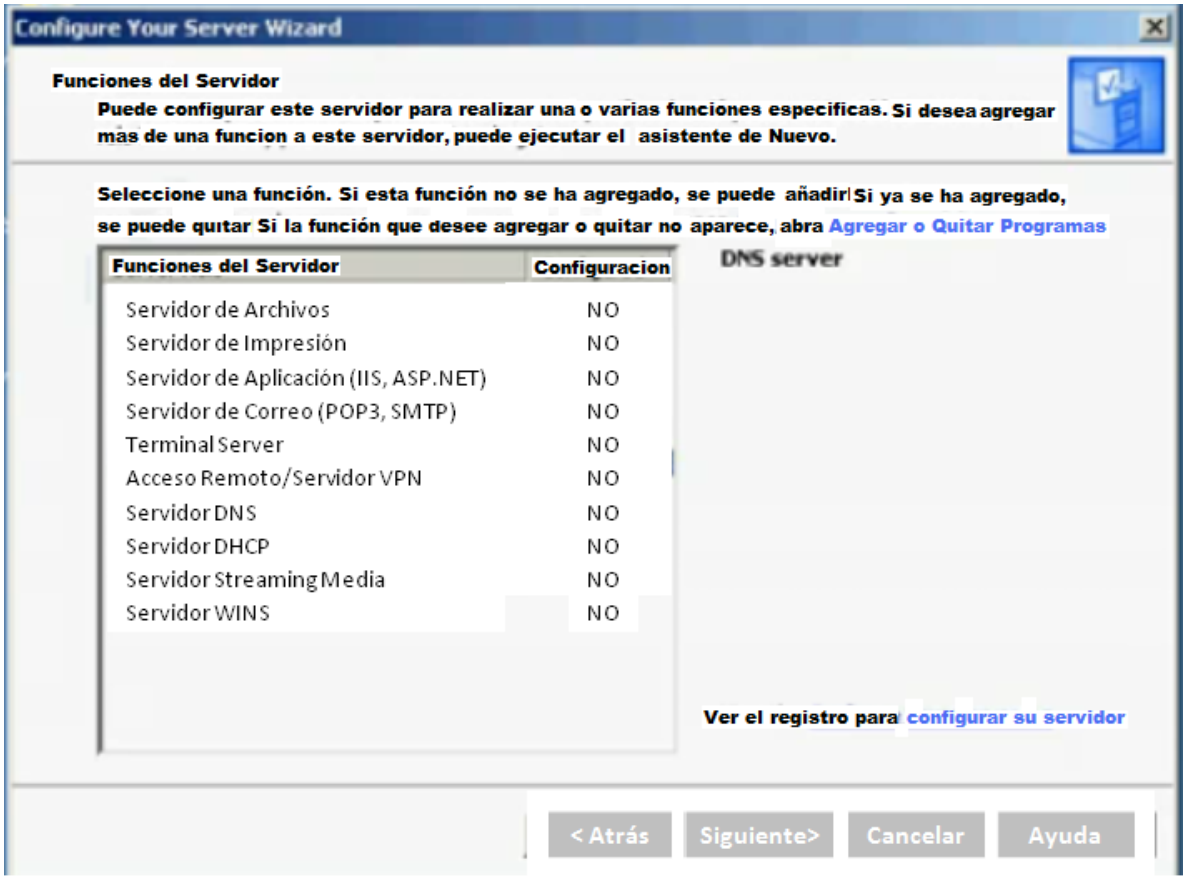
Figura 23. Agregar o quitar Función del servidor

Figura 24. Configurar el Servidor VPN



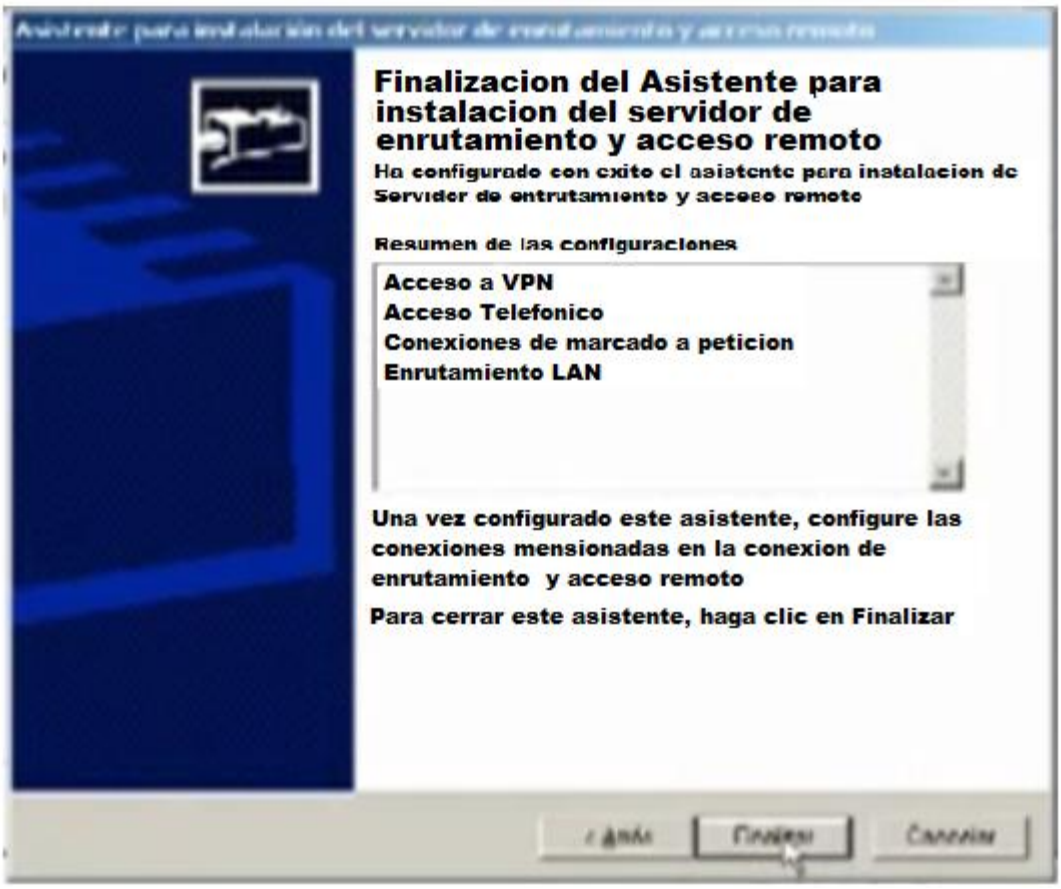
2. Aparecerá una lista de todos los servidores que trae el Server para configurar e instalar, seleccionamos ACCESO REMOTO/SERVIDOR VPN. Click en siguiente.

Figura 25. Seleccionar el Servidor VPN de una lista de servidores



3. Una vez seleccionado el Servidor VPN, se abrirá un nuevo asistente para la creación y configuración de la VPN. En la siguiente ventana elegiremos el tipo de VPN que deseamos instalar en la red. En este caso elegimos CONFIGURACION PERSONALIZADA, en la siguiente ventana seleccionar ACCESO VPN, ACCESO TELEFONICO Y ENRUTAMIENTO LAN. Click en siguiente.
4. Esta ventana muestra un resumen de toda la configuración que se realizo en la creación del Servidor VPN. Clic para finalizar el asistente de la creación del Servidor VPN

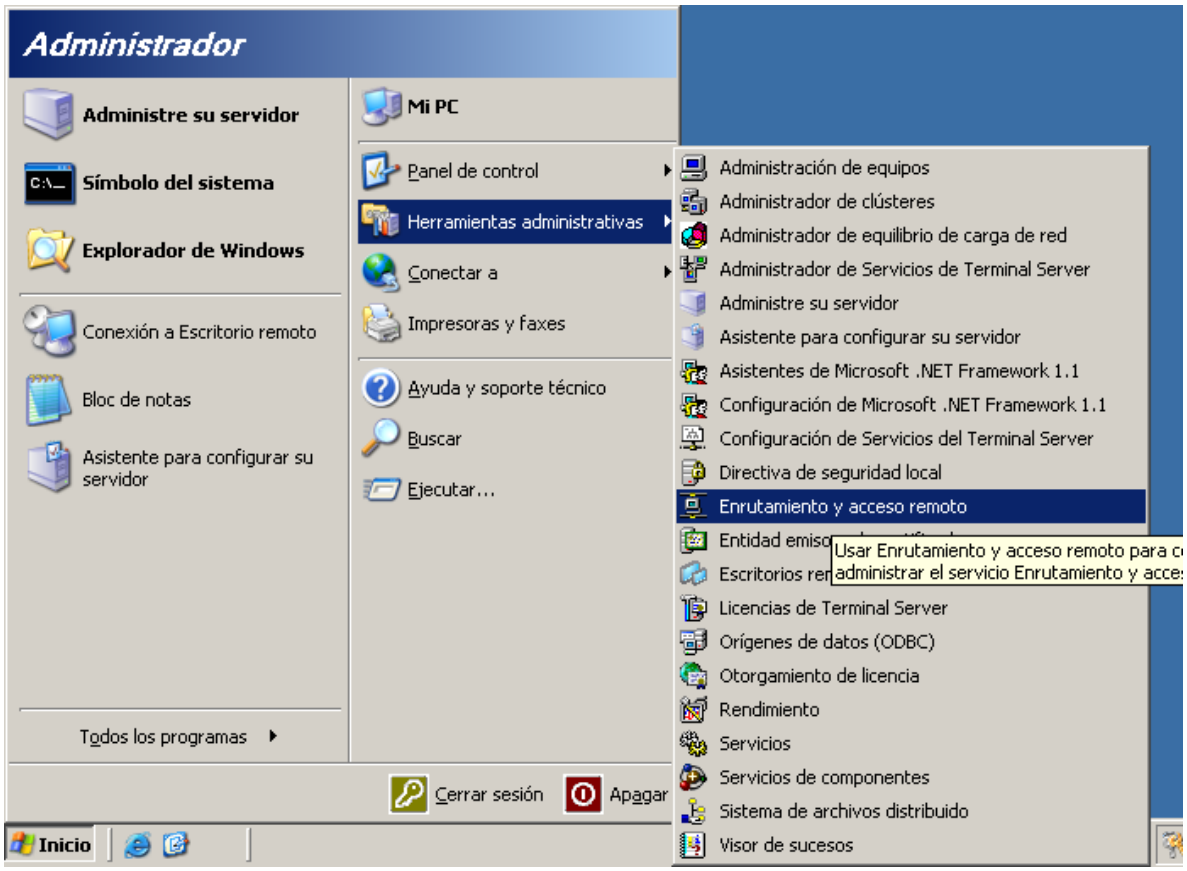
Figura 26. Resumen de la Creación del Servidor VPN.



Una vez creado el servidor VPN en Server 2003, Habilitaremos el Servicio de enrutamiento y acceso remoto del servidor:

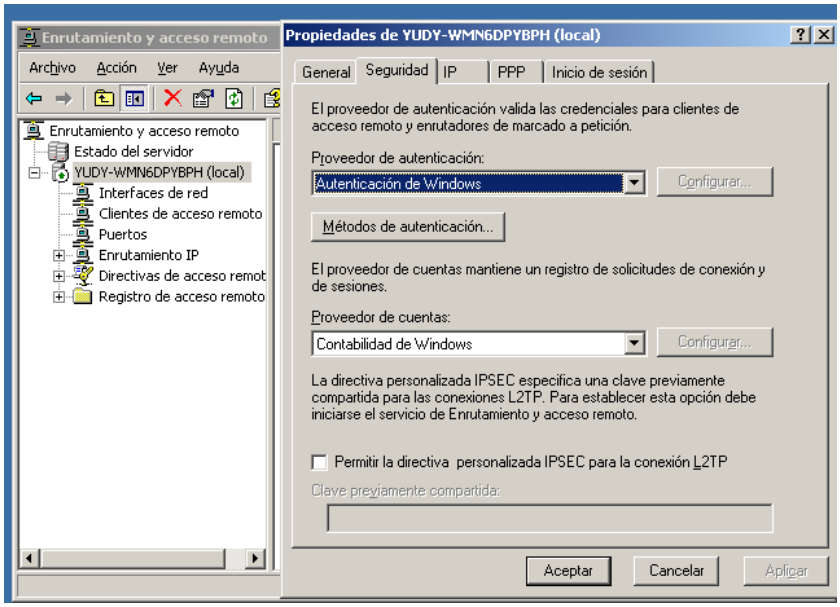
1. En el menú Herramientas administrativas, ubicamos Enrutamiento y acceso remoto, para configurar y administrar el servidor que creamos anteriormente.
En la parte izquierda de la ventana vemos el servidor VPN, damos clic derecho en el servidor en este caso se llama YUDY-WMN6DPYBPH (local) y verificamos que el proveedor de autenticación este en Autenticación de Windows en la pestaña Seguridad.

Figura 27. Administrar y configurar el Servidor VPN



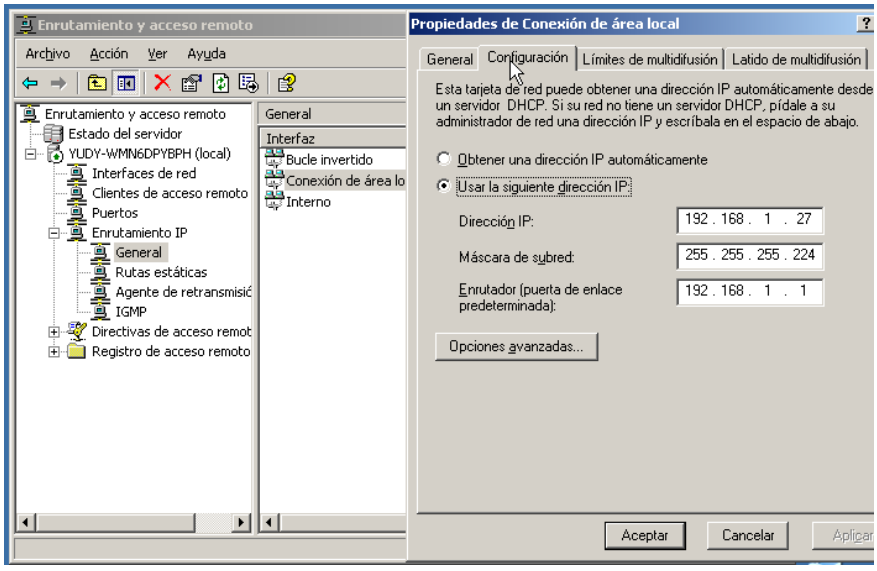
2. Click derecho a YUDY-WMN6DPYBPH (local), seleccionamos PROPIEDADES, vamos a la pestaña SEGURIDAD, damos click en la opción “permitir la directiva personalizada IPSEC para la conexión L2TP” y damos una clave previamente compartida (1234).

Figura 28. Habilitar Protocolos VPN



3. Ubicarse nuevamente en las opciones del Servidor de la parte Izquierda, seleccionamos ENRUTAMIENTO IP - GENERAL, en la parte derecha de la pantalla aparecerán una serie de conexiones, ubicamos Conexión de Área Local y con click derecho a esta opción elegimos Propiedades, esta ventana nos permitirá configurar la dirección IP del servidor. La Dir IP del servidor es la 192.168.1.27/27.

Figura 29. Configuración del Direccionamiento IP del Servidor



4. Nuevamente nos ubicamos las opciones de la parte izquierda y damos click en Puertos, seleccionamos Propiedades y verificamos que tanto el mini puerto (PPTP) como el (L2TP), tengan habilitadas conexiones de acceso remoto (solo entrada) y conexiones de enrutamiento de marcado a petición (de entrada y salida).

Figura 30. Verificación de los Puertos PPTP y L2TP

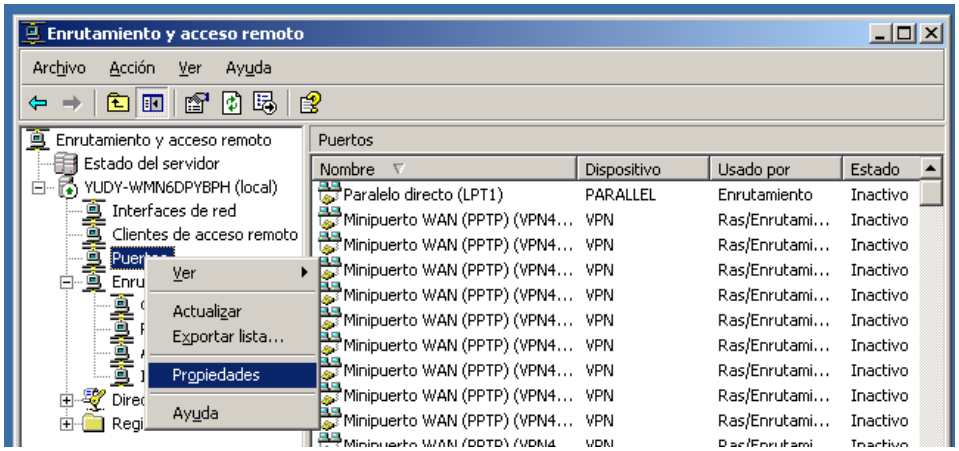
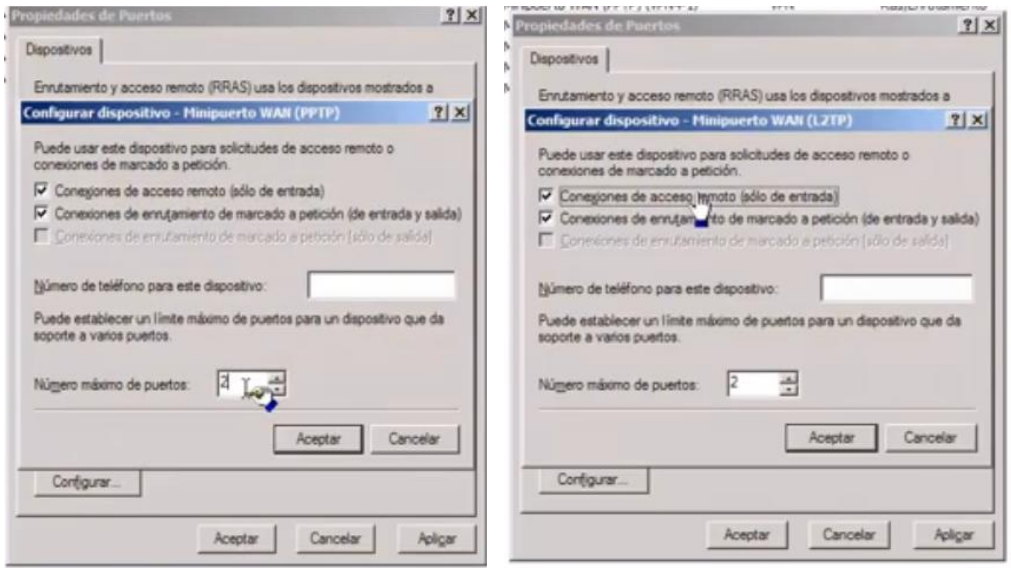
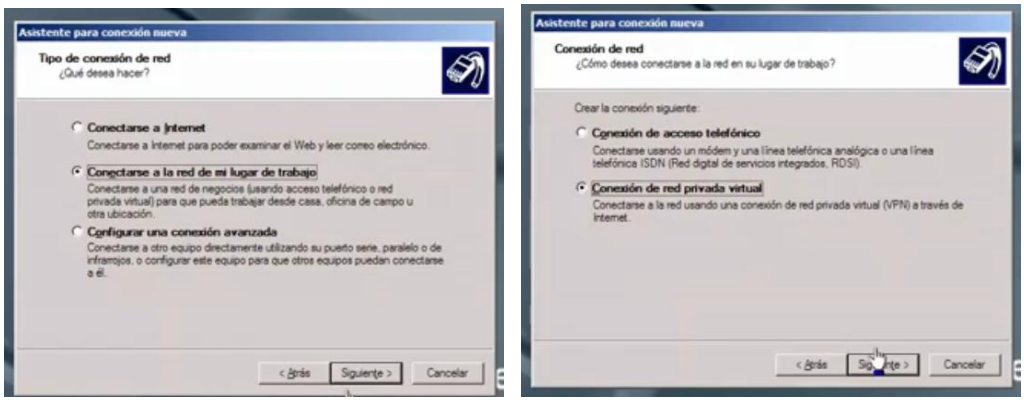


Figura 31. Cuadro de las Propiedades de los Puertos PPTP Y L2TP



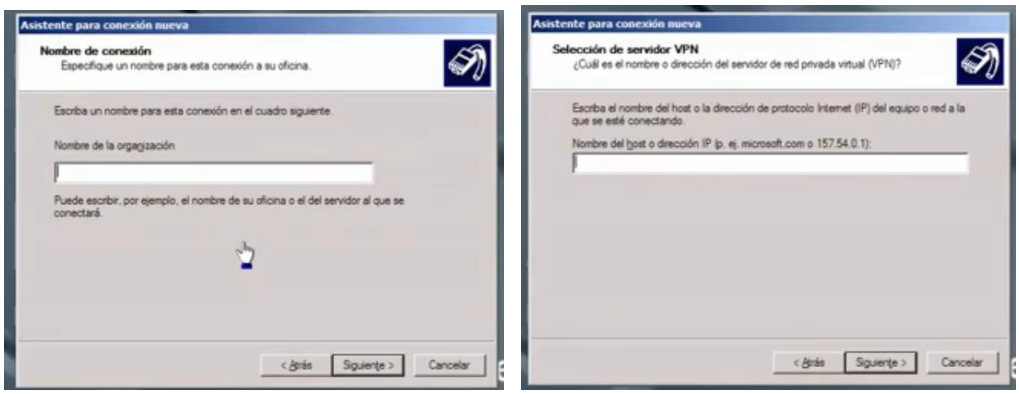
5. Ahora vamos a crear una conexión nueva, vamos a Inicio – Conexiones de Red – Crear una nueva Conexión – Conectarse a la red de mi lugar de trabajo – Conexión de Red Privada Virtual

Figura 32. Ventana de conexión nueva en Server 2003



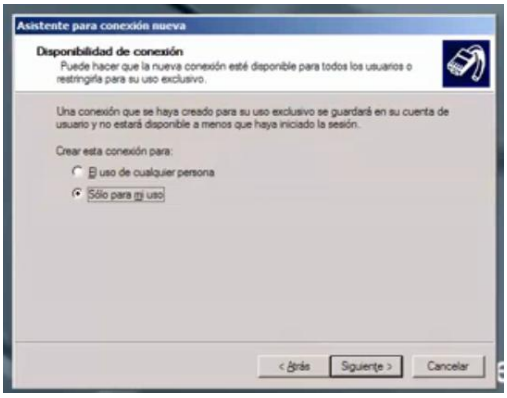
6. Nos aparecerá un cuadro en la que ingresaremos el nombre de la conexión la cual la llamaremos **Hard** y la dirección IP del servidor.

Figura 33. Ventana que permite el ingreso de los datos del servidor (Nombre y contraseña)



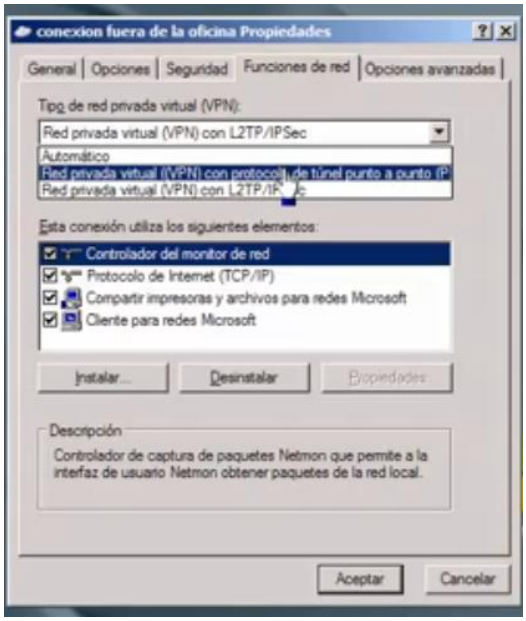
7. En la siguiente ventana seleccionamos solo para mi uso, siguiente y finalizar.

Figura 34. Habilitar el uso que se dará a la conexión nueva



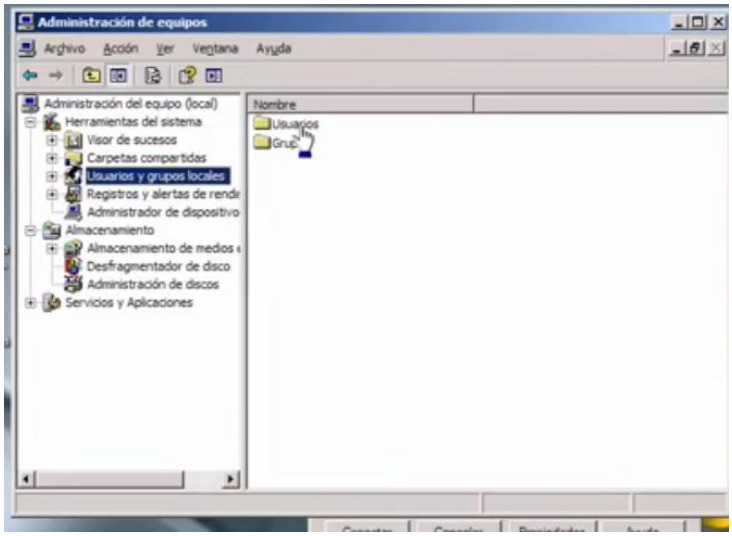
5. En la siguiente ventana damos click en Propiedades - funciones de red y seleccionamos en tipo de VPN Red Privada Virtual con protocolo de túnel puerto a puerto.

Figura 35. Configuración del Protocolo de Túnel VPN



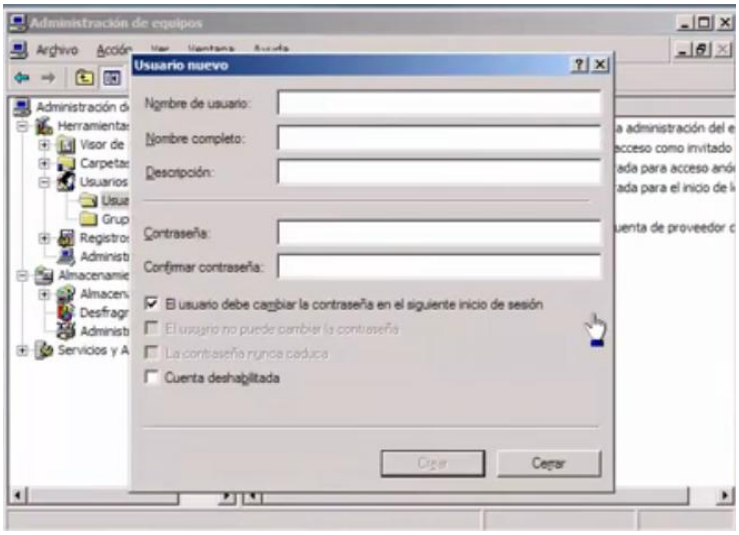
6. Una vez configurada la conexión VPN, creamos los usuarios que podrán ingresar a esta red. Click derecho a Mi PC – administrar – usuarios, en esta ventana aparecerá una lista de los usuarios que estén creados.

Figura 36.Creacion de los usuarios que podrán acceder a la conexión VPN



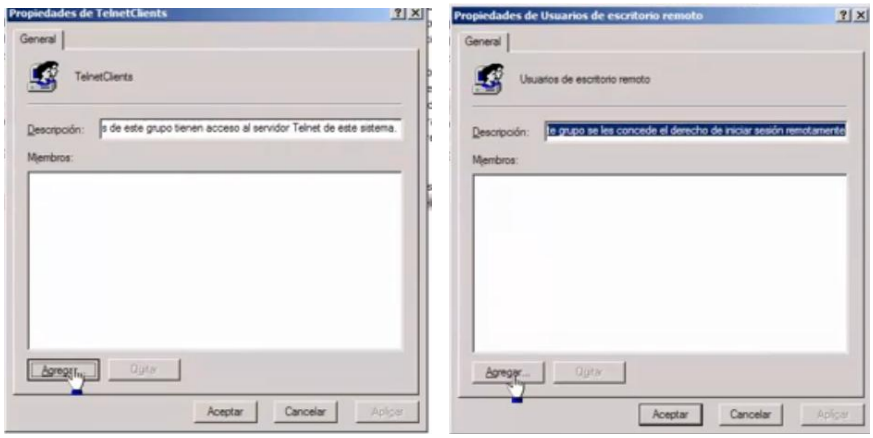
7. Para crear usuarios nuevos damos click derecho usuario Nuevo, en esta ventana ingresaremos el nombre del usuario y contraseña.

Figura 37. Configuración para un usuario nuevo



8. Una vez creado el usuario vamos a Grupos y agregamos este usuario a Telnet y usuarios de acceso remoto.

Figura 38. Habilitar privilegios de conectividad para los usuarios.



9. Vamos a Usuarios nuevamente y damos click derecho – Propiedades al usuario que creamos en la pestaña miembro usuario eliminamos la conexión Usuario, ahora vamos a la pestaña marcado y seleccionamos Permitir Acceso

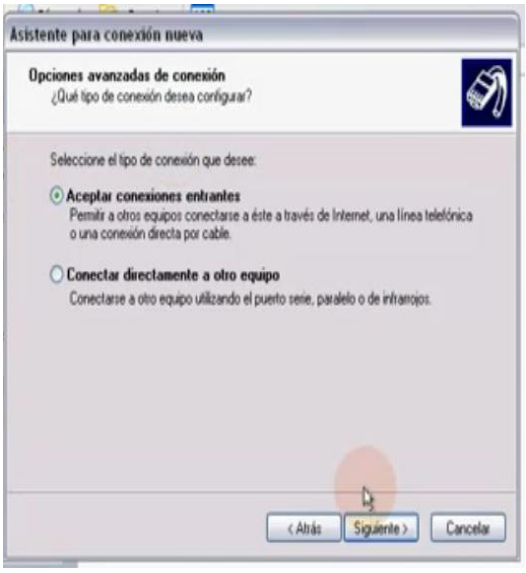
Finalmente creamos una conexión VPN en Server 2003

1. Inicio - Mis sitios de Red – en esta ventana aparecen todas las conexiones activas que tiene el equipo como por ejemplo una conexión a internet o la conexión de área local.
   En la parte izquierda de la ventana encontramos un menú, seleccionamos Crear una Conexión Nueva. Nos abrirá un asistente que nos ayudara a la creación de esta conexión.

Figura 39. Asistente para conexión server 2003

2. En la siguiente ventana damos click en Crear una conexión avanzada y siguiente. Luego seleccionamos Aceptar Conexiones Entrantes. Siguiente

Figura 40. Configuración de una conexión nueva para el Servidor VPN



3. Click en Permitir Conexiones Virtuales Privadas, siguiente. El esta ventana seleccionamos el usuario que queremos para la VPN.

Figura 41. Asignación de los usuarios que podrán conectarse a la VPN

4. Si no contamos con ningún usuario en la parte de abajo hay una opción que dice agregar, en ella podemos crear nuestro usuario. Siguiente

Figura 42. Agregar usuario Nuevo

5. En esta ventana configuraremos el rango de direcciones que serán aceptadas por la VPN. Click en Protocolo TCP/IP – Propiedades. Siguiente y Finalizar.

Figura 43. Asignación de las direcciones IP aceptadas por la VPN

3.3.2 **Configuración de VPN Cliente.**

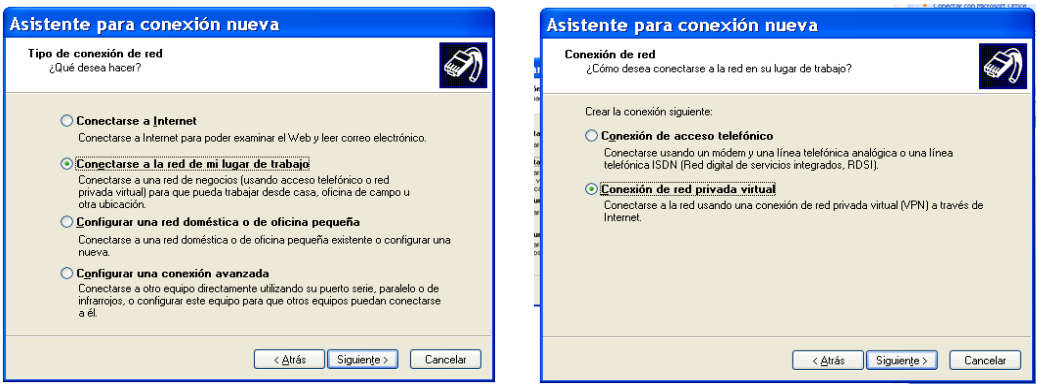
Con el fin de comunicar los equipos remotos a la LAN de cada sede, se configurara en estos la VPN Cliente, la cual permitirá la conexión con el servidor para ingresar a la red local y trabajar como si se encontrara en la empresa.
En la configuración de los equipos realizaremos los siguientes pasos de pendiendo del Windows que tenga instalado:

- ❖ Para Windows XP

1. Inicio - Mis sitios de Red – en el menú de la parte izquierda, seleccionamos Crear una Conexión Nueva. Nos abrirá un asistente para conexión nueva, siguiente.

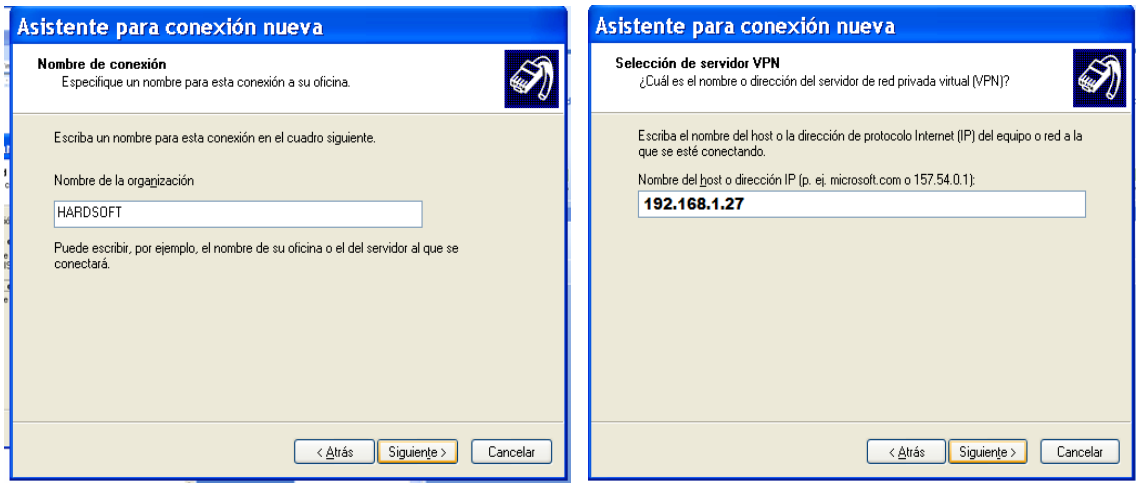
2. Seleccionamos conectarse a la red de mi trabajo, siguiente. Damos click en conexión de Red Privada Virtual. siguiente

Figura 44. Crear conexión VPN como cliente en Win XP.



3. Luego daremos un nombre a la conexión en este caso pondré Hard. Siguiente, en esta ventana nos pide ingresar la dirección IP, la cual es la dirección del servidor VPN. Siguiente y Finalizar.

Figura 45. Ingreso de los datos de la conexión (Nombre de conexión y Dirección de salida al servidor).



Cuando termina el asistente de conexión nueva, se abre automáticamente una ventana que pide nombre de usuario y contraseña, esta información es la que ingresamos en el servidor.

Figura 46. Conexión a la VPN

3.3.3. Configuración de los Puertos VPN

La primera vez que se inicia un servidor VPN, Windows 2003 crea automáticamente 128 puertos PPTP y 128 puertos L2TP. El número de puertos virtuales disponibles para un servidor VPN no está limitado por el hardware físico. Puede aumentarlo o reducirlo al número apropiado para el ancho de banda disponible en el servidor.

En Windows Server 2003, se pueden crear hasta 1.000 puertos del Protocolo de túnel punto a punto (PPTP) y hasta 1.000 puertos del Protocolo de túnel de capa 2 (L2TP). No obstante, Windows Server 2003, sólo puede aceptar una conexión de red privada virtual (VPN) cada vez. Windows Server 2003, Standard Edition, puede aceptar hasta 1.000 conexiones VPN simultáneas

Para configurar los puertos VPN, se debe realizar lo siguiente en el servidor:

1. Inicio - Enrutamiento y acceso remoto, abrir el cuadro de diálogo en la parte izquierda hay un menú, seleccionamos Propiedades de Puertos con click derecho en esta opción.
2. En el cuadro de diálogo Propiedades de Puertos, seleccionamos un dispositivo (para los puertos VPN, son Mini puerto WAN (PPTP) y Mini puerto WAN (L2TP) y haga clic en Configurar.
3. En el cuadro de diálogo Configurar dispositivo, activamos la casilla de verificación Conexiones de acceso remoto (sólo de entrada) para habilitar las conexiones VPN entrantes.
4. Opcionalmente podemos aumentar o reducir el número de puertos virtuales disponibles en el servidor.
5. Damos clic en Aceptar en los cuadros de diálogo, Configurar dispositivos y Propiedades de Puertos.

4. **CONCLUSIONES Y RECOMENDACIONES**

- El diseño de la red de Hardsoft inicia desde cero, teniendo en cuenta el sistema actual, con el fin de evitar inconsistencias a futuro. El montaje de la red se realizara mediante Packet Tracer para configurar los dispositivos de forma real, permitiendo el comportamiento y funcionamiento de los dispositivos al configurarlos y evitando inconsistencias a futuro.

- El direccionamiento IP que se realizo para Hardsoft a partir de una dirección IP, permitirá la escalabilidad y rendimiento de la red, es decir, que si la empresa sigue creciendo no tendrá inconveniente con la asignación de direcciones a equipos nuevos.

- El diseño de la red para la empresa Hardsoft S.A, permite a los usuarios trabajar de una forma sencilla, efectiva y segura, generando mayor productividad, reflejándose en la facilidad y rapidez, para la obtención de información.

- Las VPN representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos, reduciendo significativamente el costo de la transferencia de datos de un lugar a otro.

- Realizar mantenimiento periódico a nivel de hardware y software, a los equipos para evitar inconvenientes con el funcionamiento de la red tanto local como externa

- La seguridad en las redes es una necesidad, dadas las características de la información que por ellas se transmite, permitiendo la confidencialidad e integridad de dicha información mediante protocolos de encriptación que eviten la manipulación de terceros.

- Informar a los usuarios de los servicios y beneficios de la red, así como de su funcionamiento; además solicitar que se enmarquen en las políticas de seguridad establecidas.

BIBLIOGRAFIA

- *REDES* DE COMPUTADORAS Tanenbaum, Andrews S. (Prentice Hall)

- http://technet.microsoft.com/es-es/library/cc781054(WS.10).aspx

- Cisco Networking Academy, CCNA Exploration 1, Network Fundamentals, Versión 4.0, en línea. http://ev-iip.netacad.net/virtuoso/servlet/org.cli.delivery.rendering.servlet.CCServlet/LMS_ID=CNAMS,Theme=ccna3theme,Style=ccna3,Language=es,Version=1,RootID=knet-lcms_exploration1_es_40,Engine=static/CHAPID=null/RLOID=null/RIOID=null/theme/cheetah.html?cid=0600000000&l1=tl&l2=en&chapter=intro. Junio 2009

- Cisco Networking Academy, CCNA Exploration 2, Routing Protocols and Concepts, Version 4.0, en línea, http://ev-iip.netacad.net/virtuoso/servlet/org.cli.delivery.rendering.servlet.CCServlet/LMS_ID=CNAMS,Theme=ccna3theme,Style=ccna3,Language=es,Version=1,RootID=knet-lcms_exploration2_es_40,Engine=static/CHAPID=null/RLOID=null/RIOID=null/theme/cheetah.html?cid=0900000000&l1=tl&l2=en&chapter=intro. Agosto 2009

- Cisco Networking Academy, CCNA Exploration 4, Accessing the WAN, Version 4.0, en línea, http://ev-iip.netacad.net/virtuoso/servlet/org.cli.delivery.rendering.servlet.CCServlet/LMS_ID=CNAMS,Theme=ccna3theme,Style=ccna3,Language=es,Version=1,RootID=knet-lcms_exploration4_es_40,Engine=static/CHAPID=null/RLOID=null/RIOID=null/theme/cheetah.html?cid=1400000000&l1=tl&l2=en&chapter=intro. Noviembre 2009

- INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. Documentación: Citas y notas de pie de pagina, 2 ed. Bogotá: ICONTEC, 1995. 7p. (NTC 1487).

- Pérez Hernández María Gabriela. Ciencias Fundamentales y Tecnología. Editorial Dikinson. 2006.

- Tanenbaum Andrew S.. Redes de computadoras. Cuarta Edición. PEARSON EDUCACION, México, 2003.912 p. ISBN: 970-26-0162-2

ANEXO 1 CONFIGURACION ROUTER LAGO

```
hostname "LAGO"
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
imp ssh version 1
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.192
 duplex auto
 speed auto
interface FastEthernet0/1
 ip address 192.168.2.65 255.255.255.192
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
interface Serial0/2/1
 no ip address
 shutdown
interface FastEthernet1/0
 bandwidth 64000
 ip address 200.200.1.2 255.255.255.252
router ospf 1
 log-adjacency-changes
 network 200.200.1.0 0.0.0.3 area 10
 network 192.168.1.0 0.0.0.63 area 10
 ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet1/0
no cdp run
banner motd ^RLAGO, prohibido el Acceso no autorizado^C
line con 0
 password cisco
 login
line vty 0 4
 password cisco
login
end
```

ANEXO 2 ENRUTAMIENTO ROUTER LAGO

```
192.168.1.0/27 is subnetted, 4 subnets
C       192.168.1.0 is directly connected, FastEthernet0/0
O       192.168.1.33 [110/3] via 200.200.1.1, 03:08:36, FastEthernet1/0
O       192.168.1.48 [110/3] via 200.200.1.1, 03:08:36, FastEthernet1/0
O       192.168.1.64 [110/3] via 200.200.1.1, 03:08:36, FastEthernet1/0
    192.168.2.0/26 is subnetted, 3 subnets
C       200.200.1.0 is directly connected, FastEthernet1/0
O       200.200.1.4 [110/2] via 200.200.1.1, 03:08:36, FastEthernet1/0
```

ANEXO 3 CONFIGURACION ROUTER CENTRO

```
hostname "CENTRO"
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
interface FastEthernet0/0
ip address 192.168.1.32 255.255.255.240
duplex auto
speed auto
interface Serial0/0
no ip address
shutdown
interface Serial0/1
no ip address
shutdown
interface FastEthernet1/0
bandwidth 64000
ip address 200.200.1.6 255.255.255.252
router ospf 1
log-adjacency-changes
network 200.200.1.4 0.0.0.3 area 10
network 192.168.1.32 0.0.0.63 area 10
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet1/0
no cdp run
banner motd ^RCENTRO, prohibido el Acceso no autorizado^C
line con 0
password cisco
login
line vty 0 4
password cisco
login
end
```

ANEXO 4 ENRUTAMIENTO ROUTER CENTRO

```
192.168.1.0/26 is subnetted, 4 subnets
O       192.168.1.0 [110/3] via 200.200.100.5, 03:33:46, FastEthernet1/0
C       192.168.1.32 is directly connected, FastEthernet0/0
O       192.168.1.48 [110/3] via 200.200.100.5, 03:33:46, FastEthernet1/0
O       200.200.100.0 [110/2] via 200.200.100.5, 03:33:46, FastEthernet1/0
C       200.200.1.4 is directly connected, FastEthernet1/0
O       200.200.1.1 [110/2] via 200.200.100.5, 03:33:46, FastEthernet1/0
S*   0.0.0.0/0 is directly connected, FastEthernet1/0
```

ANEXO 5 CONFIGURACION ROUTER GALERIAS

```
hostname "GALERIAS"
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
interface FastEthernet0/0
ip address 192.168.1.49 255.255.255.240
duplex auto
speed auto
interface Serial0/0
no ip address
shutdown
interface Serial0/1
no ip address
shutdown
interface FastEthernet1/0
bandwidth 64000
ip address 200.200.1.10 255.255.255.252
router ospf 1
log-adjacency-changes
network 200.200.1.8 0.0.0.3 area 10
network 192.168.1.48 0.0.0.63 area 10
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet1/0
no cdp run
banner motd ^CRouter Galerias, prohibido el Acceso no autorizado^C
line con 0
password cisco
login
line vty 0 4
password cisco
login
end
```

ANEXO 6 ENRUTAMIENTO ROUTER GALERIAS

```
192.168.1.0/26 is subnetted, 4 subnets
O       192.168.1.0 [110/3] via 200.200.1.9, 03:48:28, FastEthernet1/0
O       192.168.1.1 [110/3] via 200.200.1.9, 03:48:28, FastEthernet1/0
C       192.168.1.32 is directly connected, FastEthernet0/0
200.200.1.0/30 is subnetted, 6 subnets
O       200.200.1.0 [110/2] via 200.200.1.9, 03:48:28, FastEthernet1/0
O       200.200.1.4 [110/2] via 200.200.1.9, 03:48:28, FastEthernet1/0
S*   0.0.0.0/0 is directly connected, FastEthernet1/0
```

ANEXO 7 CONFIGURACION ROUTER ISP

```
hostname ISP
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
interface FastEthernet1/0
no ip address
duplex auto
speed auto
shutdown
interface Serial2/0
no ip address
shutdown
interface Serial3/0
no ip address
shutdown
interface FastEthernet4/0
bandwidth 64000
ip address 200.200.1.1 255.255.255.252
interface FastEthernet5/0
bandwidth 64000
ip address 200.200.1.5 255.255.255.252
interface FastEthernet6/0
bandwidth 64000
ip address 200.200.1.9 255.255.255.252
router ospf 1
log-adjacency-changes
network 200.200.1.0 0.0.0.3 area 10
network 200.200.1.4 0.0.0.3 area 10
network 200.200.1.8 0.0.0.3 area 10
ip classless
no cdp run
line con 0
password cisco
login
line vty 0 4
password cisco
login
end
```

ANEXO 8 ENRUTAMIENTO DEL ROUTER ISP

```
192.168.1.0/27 is subnetted, 4 subnets
O       192.168.1.0 [110/2] via 200.200.1.2, 02:40:52, FastEthernet4/0
O       192.168.1.32 [110/2] via 200.200.1.6, 02:40:52, FastEthernet5/0
O       192.168.1.48 [110/2] via 200.200.1.10, 02:40:52, FastEthernet6/0
200.200.100.0/30 is subnetted, 6 subnets
C       200.200.1.0 is directly connected, FastEthernet4/0
C       200.200.1.4 is directly connected, FastEthernet5/0
C       200.200.1.8 is directly connected, FastEthernet6/0
```